POLÍTICA DE SEGURANÇA CIBERNÉTICA E ARMAZENAMENTO DE DADOS EM NUVEM PARA INSTITUIÇÕES DE PAGAMENTO

A Resolução BCB nº 85 dispõe sobre a política de segurança cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo BCB.

A nova Resolução entrará em vigor em **1º de agosto de 2021**.
A seguir destacamos suas principais regras.

DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Segundo a nova norma, as instituições de pagamento devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, a qual deverá ser compatível com:

- O porte, o perfil de risco e o modelo de negócio da instituição;
- A natureza das atividades da instituição e a complexidade dos produtos e serviços oferecidos; e
- A sensibilidade dos dados e das informações sob responsabilidade da instituição.

A POLÍTICA DE SEGURANÇA CIBERNÉTICA DEVE ESPECIFICAR, NO MÍNIMO:

1. Os objetivos de segurança cibernética da instituição de pagamento;
2. Os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição de pagamento a incidentes e atender aos demais objetivos de segurança cibernética;
3. Os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;
4. O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição de pagamento;
5. As diretrizes para:
   - elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;
   - a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição de pagamento;

- classificação dos dados e das informações quanto à relevância; e
- a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;

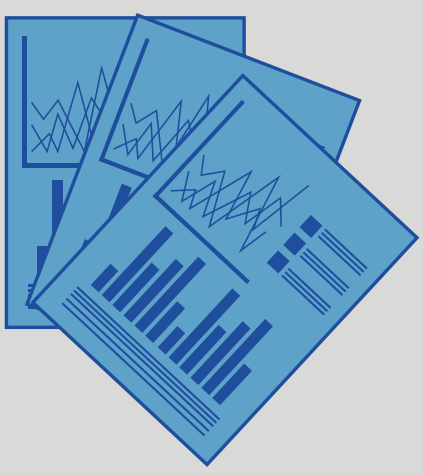
6 Os mecanismos para disseminação da cultura de segurança cibernética na instituição de pagamento, incluindo:

- a implementação de programas de capacitação e de avaliação periódica de pessoal;
- a prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos; e
- o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e

7 As iniciativas para compartilhamento de informações sobre os incidentes relevantes, mencionados no inciso IV, com as instituições de pagamento e com as demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

A **política de segurança cibernética** deve ser divulgada aos funcionários da instituição de pagamento e às empresas prestadoras de serviços a terceiros. As instituições de pagamento devem divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética.

As **instituições de pagamento** devem estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética e, também, designar diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.



Também deverá ser elaborado **relatório anual** sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro.

A POLÍTICA DE SEGURANÇA CIBERNÉTICA E O PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES DEVEM SER DOCUMENTADOS E REVISADOS, NO MÍNIMO, ANUALMENTE.

A equipe de Direito Bancário e Financeiro do Azevedo Sette Advogados se coloca à disposição para esclarecimentos adicionais sobre o tema.

POLÍTICA DE SEGURANÇA CIBERNÉTICA E ARMAZENAMENTO DE DADOS EM NUVEM PARA INSTITUIÇÕES DE PAGAMENTO

A nova Resolução BCB nº 85 entrará em vigor em **1º de agosto de 2021**.

DA CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

As instituições de pagamento devem assegurar que suas **políticas**, **estratégias** e **estruturas** para gerenciamento de riscos previstas na regulamentação em vigor, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços, contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior.
Devendo adotar procedimentos que contemplem:

I A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e

II A verificação da capacidade do potencial prestador de serviço de assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- A sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;
- O acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos usuários finais da instituição por meio de controles físicos ou lógicos; e
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da instituição.

A CONTRATAÇÃO DE SERVIÇOS RELEVANTES DE PROCESSAMENTO, ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM DEVE SER COMUNICADA PELAS INSTITUIÇÕES DE PAGAMENTO AO BCB.

QUANTO À CONTRATAÇÃO DE SERVIÇOS RELEVANTES DE PROCESSAMENTO, ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM PRESTADOS NO EXTERIOR, AS INSTITUIÇÕES DE PAGAMENTO DEVEM OBSERVAR OS SEGUINTES REQUISITOS:

I A existência de convênio para troca de informações entre o BCB e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

II A instituição de pagamento contratante deve assegurar que a prestação dos serviços referidos no caput não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do BCB;

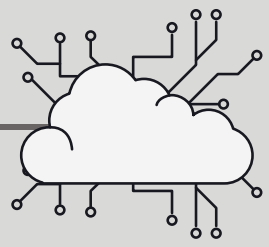
III Definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e

IV Prever alternativas para a continuidade dos serviços de pagamento prestados, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de **inexistência de convênio** nos termos do item I acima, a instituição de pagamento contratante deverá solicitar autorização do BCB para a contratação do serviço, no prazo mínimo de 60 (sessenta) dias antes da contratação.

Para atendimento aos itens II e III, as instituições deverão assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições de pagamento contratantes e do BCB aos dados e às informações.

DISPOSIÇÕES GERAIS



As instituições de pagamento devem assegurar que suas políticas previstas na estrutura de gerenciamento de riscos, disponham sobre o tratamento de incidentes relacionados com o ambiente cibernético, dos procedimentos a serem seguidos no caso da interrupção de serviços de processamento e armazenamento de dados, bem como instituir mecanismos de acompanhamento e controle.

O BCB poderá vetar ou impor restrições para a contratação desses serviços quando constatar, a qualquer tempo, a inobservância do disposto nesta Resolução, bem como a limitação à atuação do BCB, estabelecendo prazo para a adequação dos referidos serviços e dos contratos correspondentes.

A equipe de Direito Bancário e Financeiro do Azevedo Sette Advogados se coloca à disposição para esclarecimentos adicionais sobre o tema.