GRAN CONCURSOS

SEGURANÇA CIBERNÉTICA

Resolução CMN n. 4.893/2021

Presidente: Gabriel Granjeiro

Vice-Presidente: Rodrigo Calado

Diretor Pedagógico: Erico Teixeira

Diretora de Produção Educacional: Vivian Higashi

Gerência de Produção de Conteúdo: Magno Coimbra

Coordenadora Pedagógica: Élica Lopes

CÓDIGO:

230728274504

LEONARDO DEITOS

Servidor do Tribunal de Justiça de Santa Catarina, Ex-Policial Civil, Pós-graduado em Ciências Policiais e Investigação Criminal, Bacharel em Direito. Professor de Cursos Preparatórios para Concursos Públicos.

GRAN CONCURSOS

SUMÁRIO

Apresentação 4
Resolução CMN 4.893/2021 5
Introdução 5
Resolução CMN N. 4.893/2021 5
Política De Segurança Cibernética 5
Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem 9
Disposições Gerais 14
Disposições Finais. 16
Resumo 18
Exercícios 22
Gabarito 27
Gabarito Comentado. 28

APRESENTAÇÃO

Olá, querido(a) aluno(a)!

Nesta aula estudaremos um tópico crucial para o seu sucesso nos concursos públicos: a Resolução CMN 4.893/2021, que trata da segurança cibernética das instituições financeiras. Este é um tema atual e de extrema relevância, especialmente considerando o cenário em constante evolução das ameaças cibernéticas no mundo financeiro.

Antes de começarmos, quero que saiba que estou aqui para apoiá-lo em sua jornada de aprendizado. Se surgirem dúvidas ao longo da aula, não hesite em enviá-las para o "Fórum de Dúvidas". Estou à disposição para esclarecer qualquer questão que possa surgir.

Ao final da aula, disponibilizaremos um resumo conciso do conteúdo para facilitar sua revisão. Além disso, preparei questões inéditas para você praticar e aprimorar seus conhecimentos.

Sua opinião é inestimável para nós. Queremos que sua experiência de aprendizado seja a melhor possível. Portanto, após a aula, convido você a avaliar o conteúdo e a compartilhar críticas ou sugestões. Seu feedback ajuda a melhorar e adaptar nosso material às suas necessidades.

Agora, sem mais delongas, vamos ao estudo!

RESOLUÇÃO CMN 4.893/2021

INTRODUÇÃO

A Resolução 4.893/2021, emitida pelo Conselho Monetário Nacional, estabelece diretrizes importantes sobre segurança cibernética e os critérios para a contratação de serviços relacionados ao processamento e armazenamento de dados, tais como computação em nuvem.

Este regulamento é direcionado às instituições financeiras autorizadas pelo Banco Central do Brasil, destacando-se como um passo significativo no fortalecimento da segurança digital no setor financeiro do país.

A resolução enfatiza a importância de adotar práticas robustas de segurança cibernética para proteger dados sensíveis e sistemas financeiros críticos, visando minimizar riscos e garantir a estabilidade e confiabilidade desses serviços.

RESOLUÇÃO CMN N. 4.893/2021

Professor, a quem se aplica a Resolução CMN 4.893/2021?

A Resolução 4.893/2021 é de observância obrigatória para as instituições financeiras autorizadas a operar pelo Banco Central do Brasil. Importante ressaltar que esta Resolução não se aplica às instituições de pagamento, que devem seguir a regulamentação específica emitida pelo Banco Central, conforme suas atribuições legais.

Qual o objetivo da Resolução 4.893/2021?

A Resolução 4.893/2021 visa fortalecer a segurança dos dados e sistemas no setor financeiro, assegurando a **integridade** e a **confiabilidade** das operações bancárias.

POLÍTICA DE SEGURANÇA CIBERNÉTICA

As instituições financeiras autorizadas a operar pelo Banco Central do Brasil (BACEN) 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 política de segurança cibernética deve ser compatível com:

- O porte, o perfil de risco e o modelo de negócio da instituição;
- A natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição;

- A sensibilidade dos dados e das informações sob responsabilidade da instituição.

Uma observação importante é que, as instituições que operam pelo sistema cooperativo de crédito ou conglomerado prudencial podem adotar política de segurança cibernética única.

Por óbvio, a instituição sistema cooperativo de crédito ou conglomerado prudencial pode optar entre constituir política de segurança cibernética **própria** ou participar política de segurança cibernética **única.** Desse modo, as instituições que não constituírem política de segurança cibernética própria devem formalizar a opção por essa faculdade em reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição.

Admite-se a adoção de política de segurança cibernética única por:

- Conglomerado prudencial;
- Sistema cooperativo de crédito.

A política de segurança cibernética que for seguida pela instituição financeira deve conter critério mínimos, para assegurar o objetivo da Resolução 4.893/2021. Você sabe quais são eles?

A política de segurança cibernética deve contemplar, no mínimo:

- Os objetivos de segurança cibernética da instituição;
  - Na definição dos objetivos de segurança cibernética, deve ser contemplada a capacidade da instituição para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.
- Os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética;
  - Os procedimentos e os controles devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição.
  - Os procedimentos e os controles devem abranger, no mínimo:
    - a autenticação, a criptografia, a prevenção e a detecção de intrusão,
    - a prevenção de vazamento de informações,
    - a realização periódica de testes e varreduras para detecção de vulnerabilidades,
    - a proteção contra softwares maliciosos,
    - o estabelecimento de mecanismos de rastreabilidade,
    - os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.
- Os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;
- O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição;

  - O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.
- As diretrizes para:
  - a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;
  - 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;
    - As diretrizes devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria instituição.
  - a classificação dos dados e das informações quanto à relevância;
  - a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;
- Os mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:
  - a implementação de programas de capacitação e de avaliação periódica de pessoal;
  - a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros;
  - o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e
- As iniciativas para compartilhamento de informações sobre os incidentes relevantes.

Professor, a política de segurança cibernética é publicada pela instituição?

A política de segurança cibernética deve ser divulgada aos funcionários da instituição e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.

As instituições devem divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética.

PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

As instituições financeiras que operam sob a autorização do Banco Central do Brasil têm uma tarefa importante a cumprir no que diz respeito à segurança cibernética. Essas

instituições são obrigadas a criar e implementar um plano de ação e resposta a incidentes cibernéticos, garantindo assim uma maior proteção contra ameaças digitais.

O plano de ação e resposta a incidentes cibernéticos deve incluir, principalmente, três aspectos:

- **Ações de Adaptação:** As instituições devem desenvolver ações específicas para alinhar suas estruturas organizacionais e operacionais com os princípios e diretrizes estabelecidos pela política de segurança cibernética. Isso significa ajustar processos internos e práticas para fortalecer a defesa contra ataques cibernéticos.
- **Rotinas e Procedimentos de Prevenção e Resposta:** Devem ser estabelecidos procedimentos claros e controles eficazes, além da adoção de tecnologias apropriadas para prevenir e responder a incidentes cibernéticos. Esses procedimentos precisam estar em consonância com as diretrizes da política de segurança cibernética, garantindo uma resposta rápida e eficiente em caso de ataques.
- **Registro e Controle de Incidentes:** É essencial ter uma área dedicada para registrar e controlar os efeitos de incidentes cibernéticos relevantes. Esta área será responsável por monitorar e documentar quaisquer atividades suspeitas ou violações.

Além disso, cada instituição financeira precisa designar um diretor responsável pela política de segurança cibernética e pela execução do plano de ação e resposta a incidentes. É permitido que esse diretor desempenhe outras funções dentro da instituição, desde que não exista conflito de interesses.

Outro ponto crucial é a elaboração de um relatório anual sobre a implementação do plano. Este relatório deve abordar:

- A eficácia das ações implementadas;
- Um resumo dos resultados alcançados com as rotinas e procedimentos estabelecidos;
- Um registro dos incidentes cibernéticos relevantes que ocorreram;
- Os resultados dos testes de continuidade dos negócios, levando em consideração cenários de indisponibilidade ocasionados por incidentes.

Este relatório anual deve ser submetido ao comitê de risco (quando existente) e apresentado ao conselho de administração ou à diretoria da instituição até o dia 31 de março do ano seguinte ao da data-base.

É importante notar que tanto a política de segurança cibernética quanto o plano de ação e resposta a incidentes precisam ser aprovados pelo conselho de administração, ou na ausência deste, pela diretoria da instituição. Além disso, esses documentos devem ser revisados e atualizados pelo menos uma vez por ano, garantindo que as estratégias e práticas de segurança cibernética estejam sempre atualizadas e sejam eficazes.

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

As instituições financeiras que operam sob a autorização do Banco Central do Brasil enfrentam uma série de desafios e responsabilidades, especialmente ao terceirizar serviços críticos, como o processamento e armazenamento de dados e computação em nuvem. Essa tarefa não é apenas uma questão de escolher o fornecedor certo, mas também de seguir rigorosamente as regulamentações e práticas de governança corporativa.

Antes de firmar qualquer contrato para serviços de dados, é fundamental que as instituições financeiras adotem procedimentos detalhados e específicos. Esses procedimentos começam com a análise da importância do serviço a ser contratado, considerando aspectos como a criticidade do serviço e a sensibilidade dos dados envolvidos. É essencial avaliar como esses serviços afetarão a operação da instituição e a segurança das informações dos clientes.

Uma vez estabelecida a relevância do serviço, as instituições devem realizar uma verificação minuciosa do potencial prestador de serviços. Esse processo inclui a confirmação de que o prestador pode cumprir todas as leis e regulamentações aplicáveis, garantir o acesso aos dados processados ou armazenados, e assegurar a confidencialidade, integridade e recuperação desses dados. Além disso, o prestador deve fornecer relatórios de auditoria independente e demonstrar sua capacidade de gerenciar e monitorar os serviços de maneira eficaz.

Outro aspecto vital é a documentação de todos os procedimentos e verificações realizados. Esta prática não apenas garante transparência e responsabilidade, mas também serve como um registro essencial para futuras referências e auditorias.

Quando os serviços incluem a execução de aplicativos via internet, as instituições devem ter certeza de que o fornecedor implementa controles robustos para proteger contra vulnerabilidades, especialmente aquelas que podem surgir com novas versões dos aplicativos.

Por fim, as instituições financeiras devem possuir os recursos e competências necessários para gerenciar de forma adequada os serviços contratados. Isso implica não apenas na capacidade de analisar informações de maneira crítica, mas também na habilidade de utilizar recursos de gestão para monitorar continuamente a qualidade e eficiência dos serviços prestados.

Assim, a terceirização de serviços de processamento e armazenamento de dados e de computação em nuvem em instituições financeiras é uma tarefa complexa que exige uma abordagem meticulosa e estruturada. Seguindo estas diretrizes, as instituições podem assegurar que os serviços contratados sejam não apenas eficientes, mas também seguros e em conformidade com todas as regulamentações pertinentes.

Resumindo:

As instituições financeiras autorizadas a funcionar pelo Banco Central, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que contemplem:

- 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;
  - Na avaliação da relevância do serviço a ser contratado, a instituição contratante deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado, levando em conta, inclusive, a classificação.
- 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 clientes da instituição por meio de controles físicos ou lógicos;
  - a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

Os serviços de computação em nuvem abrangem a disponibilidade à instituição contratante, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;
- Implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;

- Execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

ATENÇÃO

A instituição contratante dos serviços de processamento e armazenamento de dados e de computação em nuvem é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pelas instituições financeiras ao Banco Central do Brasil.

Obs.: A comunicação deve ser realizada até dez dias após a contratação dos serviços.

A comunicação deve conter as seguintes informações:

- A denominação da empresa contratada;
- Os serviços relevantes contratados;
- A indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, no caso de contratação no exterior.

Obs.: As alterações contratuais que impliquem modificação das informações devem ser comunicadas ao Banco Central do Brasil até dez dias após a alteração contratual.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior deve observar os seguintes requisitos:

- a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
- a instituição contratante deve assegurar que a prestação dos serviços referidos no caput não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;
- a instituição contratante deve 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;
- a instituição contratante deve prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

Professor, e se não houver convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados?

Caso não haja um convênio estabelecido, a instituição que deseja contratar serviços deve obter a autorização do Banco Central do Brasil. Isso inclui duas situações principais:

- Para a contratação de um novo serviço, é necessário informar o Banco Central com uma antecedência mínima de 60 dias antes de efetivar a contratação.
- Qualquer mudança nos termos do contrato que resulte em alterações das informações previamente comunicadas ao Banco Central também deve ser notificada. Neste caso, o aviso deve ser feito com pelo menos 60 dias de antecedência em relação à data planejada para a mudança contratual.

Obs.: Importante ressaltar que 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 contratantes e do Banco Central do Brasil aos dados e às informações.

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

- a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- a adoção de medidas de segurança para a transmissão e armazenamento dos dados citados armazenados, processados e gerenciados;
- a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;
- a obrigatoriedade, em caso de extinção do contrato, de:
  - transferência dos dados ao novo prestador de serviços ou à instituição contratante;
  - exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos;
- o acesso da instituição contratante a:
  - informações fornecidas pela empresa contratada, visando a verificar o cumprimento de indicação dos países e da região em cada país, bem como adoção de medidas de segurança, onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
  - informações relativas às certificações e aos relatórios de auditoria especializada;
  - informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- a obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição;

- a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;
- a adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil;
- a obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever, para o caso da decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil:

- a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso que estejam em poder da empresa contratada;
- a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:
  - a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;
  - a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

ATENÇÃO

As explicações a respeito da contratação de serviço de processamento e armazenamento de dados e de computação em nuvem não se aplicam à contratação de sistemas operados por câmaras, por prestadores de serviços de compensação e de liquidação ou por entidades que exerçam atividades de registro ou de depósito centralizado.

DISPOSIÇÕES GERAIS

As instituições financeiras autorizadas a operar pelo Banco Central do Brasil estão sujeitas a regulamentações rigorosas, especialmente no que diz respeito à continuidade de negócios e ao gerenciamento de riscos. Essas regulamentações têm o objetivo de garantir a estabilidade e a integridade do sistema financeiro, bem como a proteção dos clientes e investidores.

Uma das principais preocupações é o tratamento de incidentes relevantes relacionados com o ambiente cibernético. Com a crescente dependência da tecnologia da informação, é essencial que as instituições financeiras estejam preparadas para lidar com ameaças cibernéticas que possam comprometer a segurança de seus sistemas e dados. Portanto, as políticas de gerenciamento de riscos devem incluir procedimentos detalhados para identificar, avaliar e responder adequadamente a esses incidentes.

Além disso, as instituições financeiras devem estabelecer procedimentos claros para o caso de interrupção de serviços relevantes de processamento, armazenamento de dados e computação em nuvem contratados de terceiros. Isso envolve a consideração de cenários que abrangem desde a substituição do provedor de serviços até o restabelecimento das operações normais da instituição. A continuidade dos serviços é fundamental para a confiança dos clientes e para a estabilidade do sistema financeiro como um todo.

Os testes de continuidade de negócios também desempenham um papel crucial nesse processo. É essencial que as instituições financeiras incorporem cenários de incidentes relevantes em seus exercícios de teste. Isso significa simular situações de crise, como ataques cibernéticos ou interrupções de serviços, para garantir que estão adequadamente preparadas para responder eficazmente a essas situações quando elas ocorrerem na realidade.

Além disso, os procedimentos de gerenciamento de riscos devem incluir medidas para mitigar os efeitos dos incidentes relevantes e para estabelecer prazos claros para o reinício ou normalização das atividades ou serviços interrompidos. A comunicação também é fundamental. As instituições financeiras devem relatar prontamente ao Banco Central do Brasil qualquer ocorrência de incidentes relevantes ou interrupções de serviços que configurem uma situação de crise, juntamente com as medidas adotadas para retomar suas operações. A definição de critérios claros para identificar situações de crise é uma parte importante desse processo.

Resumindo:

As instituições financeiras autorizadas a funcionar pelo Banco Central referidas devem assegurar que suas políticas para gerenciamento de riscos previstas na regulamentação em vigor disponham, no tocante à continuidade de negócios, sobre:

- o tratamento dos incidentes relevantes relacionados com o ambiente cibernético;

- os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da instituição;
- os cenários de incidentes considerados nos testes de continuidade de negócios.

Os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à continuidade de negócios:

- o tratamento previsto para mitigar os efeitos dos incidentes relevantes e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados;
- o prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;
- a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades. As instituições devem estabelecer e documentar os critérios que configurem uma situação de crise.

Nessa mesma frente de atuação, temos que as instituições financeiras autorizadas pelo Banco Central do Brasil têm a responsabilidade de estabelecer mecanismos de acompanhamento e controle para garantir a implementação efetiva das políticas de segurança cibernética, dos planos de ação e de resposta a incidentes, bem como dos requisitos para a contratação de serviços de processamento e armazenamento de dados e computação em nuvem.

Esses mecanismos incluem a definição de processos, testes e trilhas de auditoria para monitorar e manter a segurança cibernética. Processos claros são essenciais para orientar as ações relacionadas à segurança, enquanto os testes regulares ajudam a avaliar a eficácia das medidas adotadas. Além disso, as trilhas de auditoria são importantes para rastrear atividades e eventos relacionados à segurança.

Outro aspecto fundamental é a definição de métricas e indicadores apropriados. Essas métricas permitem medir o desempenho das medidas de segurança cibernética e identificar áreas que necessitam de melhorias. Quando deficiências são identificadas, as instituições devem tomar medidas corretivas imediatas.

É importante notar que esses mecanismos também devem ser aplicados quando a instituição recebe notificações sobre a subcontratação de serviços relevantes. A auditoria interna, quando aplicável, deve realizar testes periódicos compatíveis com os controles internos da instituição para avaliar a eficácia desses mecanismos.

Além disso, as instituições financeiras são incentivadas a desenvolver iniciativas de compartilhamento de informações sobre incidentes relevantes, mesmo mantendo o dever de sigilo e respeitando a livre concorrência. Isso inclui o compartilhamento de informações sobre incidentes recebidas de empresas prestadoras de serviços a terceiros. Tais informações compartilhadas devem ser disponibilizadas ao Banco Central do Brasil. O compartilhamento de informações desempenha um papel crucial na detecção precoce e na resposta eficaz a ameaças cibernéticas em constante evolução, contribuindo assim para a segurança cibernética do setor financeiro.

De forma simplificada:

As instituições financeiras autorizadas a funcionar pelo Banco Central devem instituir mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo:

- a definição de processos, testes e trilhas de auditoria;
- a definição de métricas e indicadores adequados; e
- a identificação e a correção de eventuais deficiências.

Os mecanismos acima expostos devem:

- Ser considerados quando recebidas notificações sobre a subcontratação de serviços relevantes;
- Ser submetidos a testes periódicos pela auditoria interna, quando aplicável, compatíveis com os controles internos da instituição.

DISPOSIÇÕES FINAIS

Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

- o documento relativo à política de segurança cibernética;
- a ata de reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição, no caso de ser formalizada a opção de política de segurança cibernética única;
- o documento relativo ao plano de ação e de resposta a incidentes;
- o relatório anual;
- a documentação sobre os procedimentos de contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
- a documentação sobre os procedimentos de contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, **no caso de serviços prestados no exterior**;

- os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, contado o prazo a partir da extinção do contrato;
- os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle, contado o prazo a partir da implementação dos citados mecanismos;
- a documentação com os critérios que configurem uma situação de crise.

O Banco Central do Brasil poderá adotar as medidas necessárias para cumprimento do disposto na Resolução CMN 4.893/2021, bem como estabelecer:

- os requisitos e os procedimentos para o compartilhamento de informações;
- a exigência de certificações e outros requisitos técnicos a serem requeridos das empresas contratadas, pela instituição financeira contratante, na prestação dos serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
- os prazos máximos para reinício ou normalização das atividades ou dos serviços relevantes interrompidos;
- os requisitos técnicos e procedimentos operacionais a serem observados pelas instituições para o cumprimento da Resolução CMN 4.893/2021.

ATENÇÃO

O Banco Central do Brasil poderá vetar ou impor restrições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constatar, a qualquer tempo, a inobservância do disposto na Resolução CMN 4.893/2021, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação dos referidos serviços.

RESUMO

- Aplicação da Resolução CMN 4.893/2021:
  - Aplica-se às instituições financeiras autorizadas pelo Banco Central do Brasil.
  - Não se aplica às instituições de pagamento, que seguem regulamentação específica do Banco Central.
- Objetivo da Resolução:
  - Fortalecer a segurança de dados e sistemas no setor financeiro.
  - Assegurar a integridade e confiabilidade das operações bancárias.
- Política de Segurança Cibernética:
  - Deve ser implementada e mantida pelas instituições financeiras autorizadas pelo Banco Central.
  - Deve ser baseada em princípios que garantam confidencialidade, integridade e disponibilidade dos dados e sistemas de informação.
  - Deve ser compatível com o porte, perfil de risco, modelo de negócio e sensibilidade dos dados da instituição.
- Opção de Política Única:
  - Instituições do sistema cooperativo de crédito ou conglomerado prudencial podem adotar uma política de segurança cibernética única.
- Conteúdo Mínimo da Política:
  - Objetivos de segurança cibernética.
  - Procedimentos e controles para reduzir vulnerabilidades e atender aos objetivos de segurança cibernética.
  - Controles específicos para segurança de informações sensíveis.
  - Registro, análise e controle de incidentes relevantes.
  - Diretrizes para elaboração de cenários de incidentes e procedimentos para empresas prestadoras de serviços a terceiros.
  - Mecanismos para disseminação da cultura de segurança cibernética na instituição.
  - Iniciativas de compartilhamento de informações sobre incidentes relevantes.
- Publicação da Política:
  - Deve ser divulgada internamente aos funcionários e empresas prestadoras de serviços a terceiros.
  - Resumo das linhas gerais da política deve ser divulgado ao público.
- Plano de Ação e Resposta a Incidentes Cibernéticos:
  - Instituições financeiras autorizadas pelo Banco Central devem criar e implementar um plano de ação e resposta a incidentes cibernéticos.

  - O plano deve incluir três aspectos principais: Ações de Adaptação, Rotinas e Procedimentos de Prevenção e Resposta, e Registro e Controle de Incidentes.
  - Ações de Adaptação visam alinhar estruturas organizacionais e operacionais com a política de segurança cibernética.
  - Rotinas e Procedimentos de Prevenção e Resposta estabelecem procedimentos claros e controles eficazes para prevenir e responder a incidentes cibernéticos.
  - Registro e Controle de Incidentes envolvem o monitoramento e documentação de atividades suspeitas ou violações.
- Responsabilidades e Diretor Responsável:
  - Cada instituição financeira deve designar um diretor responsável pela política de segurança cibernética e pela execução do plano.
  - Esse diretor pode desempenhar outras funções, desde que não haja conflito de interesses.
- Relatório Anual:
  - As instituições devem elaborar um relatório anual sobre a implementação do plano de ação.
  - O relatório deve incluir a eficácia das ações implementadas, resultados das rotinas e procedimentos, registro de incidentes relevantes e resultados de testes de continuidade dos negócios.
  - Deve ser submetido ao comitê de risco (se existir) e apresentado ao conselho de administração ou diretoria até 31 de março do ano seguinte ao da data-base.
- Aprovação e Atualização:
  - A política de segurança cibernética e o plano de ação e resposta a incidentes devem ser aprovados pelo conselho de administração ou diretoria da instituição.
  - Esses documentos devem ser revisados e atualizados pelo menos uma vez por ano para garantir sua eficácia e atualização constante.
- Contratação de Serviços de Processamento e Armazenamento de Dados e Computação em Nuvem:
  - Instituições financeiras autorizadas pelo Banco Central devem seguir procedimentos detalhados antes de contratar tais serviços.
- Avaliação da Relevância do Serviço:
  - Deve considerar a criticidade do serviço e a sensibilidade dos dados envolvidos.
  - Avaliar como os serviços afetarão a operação da instituição e a segurança das informações dos clientes.
- Verificação do Prestador de Serviços:
  - O prestador deve cumprir todas as leis e regulamentações aplicáveis.
  - Deve garantir o acesso aos dados processados ou armazenados.

  - Deve assegurar confidencialidade, integridade, disponibilidade e recuperação dos dados.
  - Fornecer relatórios de auditoria independente e capacidade de gerenciar e monitorar eficazmente os serviços.
- Documentação:
  - Todas as verificações e procedimentos devem ser documentados para transparência e responsabilidade.
- Serviços com Aplicativos pela Internet:
  - Deve garantir que o fornecedor implementa controles robustos para proteger contra vulnerabilidades, especialmente com novas versões de aplicativos.
- Recursos de Gerenciamento:
  - A instituição deve possuir recursos e competências para gerenciar adequadamente os serviços contratados.
- Contratação no Exterior:
  - Deve haver convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços serão prestados.
  - A instituição deve garantir que a legislação dos países não restrinja o acesso aos dados.
- Comunicação ao Banco Central:
  - Deve ser feita até dez dias após a contratação dos serviços, informando a empresa contratada, os serviços contratados e a região onde serão prestados.
- Alterações Contratuais:
  - Alterações nas informações previamente comunicadas também devem ser notificadas até dez dias após a alteração.
- Responsabilidades da Instituição Contratante:
  - A instituição é responsável pela confiabilidade, integridade, disponibilidade, segurança e sigilo dos serviços contratados, bem como pelo cumprimento das leis e regulamentações.
- Decretação de Regime de Resolução:
  - Em caso de regime de resolução da instituição contratante pelo Banco Central, a empresa contratada deve conceder acesso irrestrito ao responsável pelo regime.
  - Deve notificar o responsável com antecedência em caso de interrupção dos serviços, aceitando pedidos de prazo adicional.
- Exceção para Sistemas Operados por Câmaras e Entidades de Compensação e Liquidação:
  - As regras não se aplicam à contratação de sistemas operados por câmaras, entidades de compensação e liquidação ou entidades de registro ou depósito centralizado.

- Segurança Cibernética e Continuidade de Negócios:
  - Instituições financeiras autorizadas pelo Banco Central devem cumprir regulamentações rigorosas relacionadas à segurança cibernética e continuidade de negócios.
- Tratamento de Incidentes Relevantes:
  - Políticas de gerenciamento de riscos devem incluir procedimentos detalhados para identificar, avaliar e responder a incidentes cibernéticos relevantes.
- Interrupção de Serviços Contratados:
  - Procedimentos claros devem ser estabelecidos para o caso de interrupção de serviços relevantes contratados de terceiros.
  - Deve incluir cenários de substituição do provedor de serviços e retomada das operações normais.
- Testes de Continuidade de Negócios:
  - Testes devem incorporar cenários de incidentes relevantes, como ataques cibernéticos e interrupções de serviços.
- Mitigação de Efeitos:
  - Procedimentos de gerenciamento de riscos devem incluir medidas para mitigar os efeitos dos incidentes relevantes.
- Comunicação ao Banco Central:
  - As instituições devem relatar prontamente ao Banco Central qualquer incidente relevante ou interrupção de serviços que configurem uma situação de crise.
- Mecanismos de Acompanhamento e Controle:
  - Devem ser estabelecidos mecanismos para monitorar e manter a segurança cibernética, incluindo processos, testes e trilhas de auditoria.
  - Métricas e indicadores devem ser definidos para medir o desempenho das medidas de segurança cibernética.
  - A auditoria interna deve realizar testes periódicos para avaliar a eficácia desses mecanismos.
- Compartilhamento de Informações:
  - As instituições são incentivadas a compartilhar informações sobre incidentes relevantes, respeitando o sigilo e a livre concorrência.
  - Isso contribui para a detecção precoce e resposta eficaz a ameaças cibernéticas em constante evolução no setor financeiro.

EXERCÍCIOS

001. (INÉDITA/2023) De acordo com a Resolução CMN N. 4.893/2021, quais são os fatores que devem ser considerados pelas instituições financeiras ao implementar uma política de segurança cibernética?
a) O porte, a localização geográfica e a infraestrutura tecnológica da instituição.
b) O perfil de risco, a natureza das operações e a sensibilidade dos dados sob responsabilidade da instituição.
c) A complexidade dos processos, a quantidade de clientes e a presença internacional da instituição.
d) O modelo de negócio, o porte e a diversificação de produtos e serviços oferecidos.

002. (INÉDITA/2023) Segundo a Resolução CMN N. 4.893/2021, que instituições podem adotar uma política de segurança cibernética única?
a) Todas as instituições financeiras, independentemente de seu porte e natureza.
b) Apenas instituições financeiras internacionais com operações no Brasil.
c) Conglomerado prudencial e sistema cooperativo de crédito.
d) Instituições financeiras com operações exclusivamente digitais.

003. (INÉDITA/2023) Conforme estabelecido pela Resolução CMN N. 4.893/2021, qual dos seguintes elementos NÃO é um requisito obrigatório para a política de segurança cibernética de uma instituição financeira?
a) Procedimentos e controles para prevenção e tratamento de incidentes cibernéticos.
b) Registro e análise detalhada da causa e impacto de incidentes cibernéticos.
c) Implementação de sistemas de informação seguros e adoção de novas tecnologias.
d) Políticas específicas para gerenciamento de mídias sociais e marketing digital.

004. (INÉDITA/2023) Segundo a Resolução CMN N. 4.893/2021, quais são as diretrizes que as instituições financeiras devem seguir em relação à disseminação da cultura de segurança cibernética?
a) Implementação de firewalls e sistemas anti-malware.
b) Capacitação e avaliação periódica do pessoal, informação aos clientes sobre precauções, e comprometimento da alta administração.
c) Parcerias com instituições governamentais para compartilhamento de informações.
d) Contratação de consultorias especializadas em segurança cibernética.

005. (INÉDITA/2023) De acordo com a Resolução CMN N. 4.893/2021, qual é o propósito da divulgação da política de segurança cibernética para os funcionários das instituições financeiras e para as empresas prestadoras de serviços a terceiros?

a) Assegurar que todos os funcionários e prestadores de serviços estejam cientes das penalidades por não cumprimento da política.
b) Promover a conscientização e garantir que a política seja implementada de forma eficaz, usando linguagem clara e acessível.
c) Oferecer treinamento detalhado em segurança cibernética a todos os funcionários e prestadores de serviços.
d) Divulgar os detalhes técnicos da política de segurança cibernética a todos os funcionários e prestadores de serviços.

006. (INÉDITA/2023) Qual deve ser o conteúdo mínimo do plano de ação e resposta a incidentes estabelecido pelas instituições financeiras, segundo a Resolução CMN N. 4.893/2021?
a) Planos detalhados de recuperação de desastres e backups regulares de dados.
b) Ações para adequação à política de segurança cibernética, rotinas de prevenção e resposta a incidentes, e área responsável pelo controle dos efeitos de incidentes.
c) Estratégias para gerenciamento de mídias sociais e comunicação em caso de vazamento de dados.
d) Procedimentos para auditoria regular e avaliação de riscos cibernéticos.

007. (INÉDITA/2023) Conforme a Resolução CMN N. 4.893/2021, quais aspectos devem ser considerados pelas instituições financeiras ao contratar serviços de processamento e armazenamento de dados e de computação em nuvem?
a) Apenas o custo e a eficiência dos serviços de processamento e armazenamento de dados.
b) A conformidade com a legislação, a integridade dos dados, e a capacidade de auditoria do prestador de serviço.
c) A localização geográfica dos servidores e a popularidade do provedor de serviços de nuvem.
d) O impacto ambiental dos data centers e a política de responsabilidade social do prestador de serviço.

008. (INÉDITA/2023) De acordo com o Art. 12 da Resolução CMN N. 4.893/2021, quais são os procedimentos prévios necessários antes da contratação de serviços de computação em nuvem por instituições financeiras?
a) Avaliação da reputação do prestador de serviços e comparação de preços no mercado.
b) Análise da capacidade do prestador de serviço em assegurar a segurança e recuperação dos dados, e verificação da aderência a certificações exigidas.
c) Consulta pública para opiniões de consumidores e análise de tendências de mercado.
d) Verificação de antecedentes criminais dos diretores do prestador de serviço e análise de balanço financeiro da empresa.

009. (INÉDITA/2023) Qual é o procedimento exigido pela Resolução CMN N. 4.893/2021 em relação à comunicação com o Banco Central do Brasil após a contratação de serviços de computação em nuvem por instituições financeiras?
a) Não há necessidade de comunicação com o Banco Central do Brasil.
b) Comunicar ao Banco Central do Brasil dentro de dez dias após a contratação, incluindo informações sobre a empresa contratada, os serviços contratados, e a localização dos dados.
c) Apresentar um relatório anual detalhado ao Banco Central do Brasil sobre todos os serviços contratados.
d) Informar ao Banco Central do Brasil apenas no caso de contratação de serviços internacionais.

010. (INÉDITA/2023) De acordo com a Resolução CMN N. 4.893/2021, quais são as responsabilidades das instituições financeiras ao contratar serviços de computação em nuvem?
a) Garantir apenas o cumprimento da legislação e regulamentação em vigor.
b) Focar exclusivamente na eficiência operacional e na redução de custos.
c) Assegurar a confiabilidade, integridade, disponibilidade, segurança e sigilo dos serviços, além do cumprimento da legislação e regulamentação.
d) Delegar todas as responsabilidades ao prestador de serviço de computação em nuvem.

011. (INÉDITA/2023) Quais são os requisitos estabelecidos pela Resolução CMN N. 4.893/2021 para a contratação de serviços de processamento, armazenamento de dados e computação em nuvem prestados no exterior por instituições financeiras?
a) Contratar apenas serviços localizados em países com acordos comerciais preferenciais com o Brasil.
b) Assegurar convênio para troca de informações, não prejudicar o funcionamento da instituição, definir locais específicos para prestação de serviços e prever alternativas de continuidade dos negócios.
c) Focar exclusivamente em serviços oferecidos por empresas multinacionais reconhecidas.
d) Garantir que os serviços sejam prestados unicamente em países com sistemas financeiros similares ao do Brasil.

012. (INÉDITA/2023) Em caso de inexistência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras do país onde os serviços de computação em nuvem serão prestados, qual procedimento deve ser seguido, segundo a Resolução CMN N. 4.893/2021?
a) A instituição financeira deve imediatamente interromper a contratação do serviço.
b) Deve ser solicitada autorização do Banco Central do Brasil com antecedência mínima de sessenta dias da contratação ou alteração contratual.
c) A instituição financeira deve estabelecer seu próprio convênio com as autoridades locais.
d) É necessário realizar uma consulta pública antes de prosseguir com a contratação.

013. (INÉDITA/2023) De acordo com a Resolução CMN N. 4.893/2021, o que deve ser especificado nos contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem?
a) A localização exata dos servidores e a lista completa de clientes da empresa contratada.
b) Apenas a duração do contrato e os termos financeiros.
c) A indicação dos países e regiões onde os serviços serão prestados e os dados armazenados, processados e gerenciados.
d) Exclusivamente as medidas de segurança cibernética adotadas pela empresa contratada.

014. (INÉDITA/2023) Segundo a Resolução CMN N. 4.893/2021, qual deve ser a ação da empresa contratada em caso de extinção do contrato de serviços de computação em nuvem?
a) Manter os dados armazenados indefinidamente.
b) Transferir os dados ao novo prestador de serviços ou à instituição contratante e depois excluí-los.
c) Vender os dados para terceiros como ativos da empresa.
d) Arquivar os dados em um sistema de armazenamento externo.

015. (INÉDITA/2023) O que está estipulado na Resolução CMN N. 4.893/2021 sobre o acesso do Banco Central do Brasil a informações relacionadas a serviços de computação em nuvem contratados por instituições financeiras?
a) O Banco Central do Brasil não tem permissão para acessar essas informações.
b) Acesso restrito apenas aos dados financeiros da instituição contratante.
c) Permissão para acessar contratos, documentações, dados armazenados e códigos de acesso.
d) Acesso somente em casos de investigações financeiras.

016. (INÉDITA/2023) Quais serviços estão isentos das obrigações estipuladas nos artigos 11 a 17 da Resolução CMN N. 4.893/2021?
a) Serviços de telecomunicações e serviços de internet.
b) Sistemas operados por câmaras, prestadores de serviços de compensação e liquidação, ou entidades de registro ou depósito centralizado.
c) Todos os serviços de consultoria financeira.
d) Serviços de segurança física e vigilância.

017. (INÉDITA/2023) Conforme a Resolução CMN N. 4.893/2021, quais aspectos devem ser abordados nas políticas de gerenciamento de riscos das instituições financeiras em relação à continuidade dos negócios?

a) Tratamento de incidentes cibernéticos, procedimentos para interrupção de serviços de TI e cenários para testes de continuidade de negócios.
b) Políticas de investimento e estratégias de marketing digital.
c) Estratégias de recrutamento de pessoal e políticas de remuneração.
d) Planos de expansão internacional e parcerias com outras instituições financeiras.

018. (INÉDITA/2023) De acordo com a Resolução CMN N. 4.893/2021, qual é o procedimento exigido das instituições financeiras em caso de incidentes relevantes ou interrupção de serviços de computação em nuvem?
a) Comunicação imediata ao Banco Central do Brasil e documentação detalhada das providências para o reinício das atividades.
b) Notificação apenas aos clientes afetados e manutenção de sigilo absoluto.
c) Comunicação exclusiva aos acionistas e investidores da instituição.
d) Suspensão imediata de todas as operações financeiras até resolução completa do incidente.

GABARITO

1. b
2. c
3. d
4. b
5. b
6. b
7. b
8. b
9. b
10. c
11. b
12. b
13. c
14. b
15. c
16. b
17. a
18. a

GABARITO COMENTADO

001. (INÉDITA/2023) De acordo com a Resolução CMN N. 4.893/2021, quais são os fatores que devem ser considerados pelas instituições financeiras ao implementar uma política de segurança cibernética?

a) O porte, a localização geográfica e a infraestrutura tecnológica da instituição.

b) O perfil de risco, a natureza das operações e a sensibilidade dos dados sob responsabilidade da instituição.

c) A complexidade dos processos, a quantidade de clientes e a presença internacional da instituição.

d) O modelo de negócio, o porte e a diversificação de produtos e serviços oferecidos.

a) Errada. A localização geográfica e a infraestrutura tecnológica não são mencionadas na resolução.

b) Certa. Reflete o Art. 2º, § 1º da resolução, que aborda o perfil de risco, natureza das operações e a sensibilidade dos dados.

c) Errada. A quantidade de clientes e a presença internacional não são critérios explicitados na resolução.

d) Errada. Apesar de mencionar o modelo de negócio e o porte, a diversificação de produtos e serviços não é um critério específico da resolução.

Letra b.

---

002. (INÉDITA/2023) Segundo a Resolução CMN N. 4.893/2021, que instituições podem adotar uma política de segurança cibernética única?

a) Todas as instituições financeiras, independentemente de seu porte e natureza.

b) Apenas instituições financeiras internacionais com operações no Brasil.

c) Conglomerado prudencial e sistema cooperativo de crédito.

d) Instituições financeiras com operações exclusivamente digitais.

a) Errada. A resolução não permite que todas as instituições financeiras adotem uma política única indiscriminadamente.

b) Errada. A resolução não faz uma distinção específica para instituições financeiras internacionais.

c) Certa. De acordo com o Art. 2º, § 2º da resolução, conglomerado prudencial e sistema cooperativo de crédito podem adotar uma política única.

d) Errada. A resolução não faz referência específica a instituições com operações exclusivamente digitais.

Letra c.

---

003. (INÉDITA/2023) Conforme estabelecido pela Resolução CMN N. 4.893/2021, qual dos seguintes elementos NÃO é um requisito obrigatório para a política de segurança cibernética de uma instituição financeira?

a) Procedimentos e controles para prevenção e tratamento de incidentes cibernéticos.

b) Registro e análise detalhada da causa e impacto de incidentes cibernéticos.

c) Implementação de sistemas de informação seguros e adoção de novas tecnologias.

d) Políticas específicas para gerenciamento de mídias sociais e marketing digital.

a) Errada. A resolução exige procedimentos e controles para prevenção e tratamento de incidentes cibernéticos (Art. 3º, II).

b) Errada. É obrigatório o registro e análise detalhada da causa e impacto de incidentes cibernéticos (Art. 3º, IV).

c) Errada. A resolução demanda a implementação de sistemas de informação seguros e a adoção de novas tecnologias (Art. 3º, § 3º).

d) Certa. A resolução não menciona políticas específicas para gerenciamento de mídias sociais e marketing digital.

Letra d.

---

004. (INÉDITA/2023) Segundo a Resolução CMN N. 4.893/2021, quais são as diretrizes que as instituições financeiras devem seguir em relação à disseminação da cultura de segurança cibernética?

a) Implementação de firewalls e sistemas anti-malware.

b) Capacitação e avaliação periódica do pessoal, informação aos clientes sobre precauções, e comprometimento da alta administração.

c) Parcerias com instituições governamentais para compartilhamento de informações.

d) Contratação de consultorias especializadas em segurança cibernética.

a) Errada. A resolução não especifica a implementação de firewalls e sistemas anti-malware como parte da cultura de segurança cibernética.

b) Certa. A resolução destaca a capacitação e avaliação periódica do pessoal, informação aos clientes e comprometimento da alta administração (Art. 3º, VI).

c) Errada. Embora importante, parcerias com instituições governamentais não são especificadas na resolução.
d) Errada. A contratação de consultorias não é uma diretriz mencionada na resolução para a disseminação da cultura de segurança cibernética.
Letra b.

---

005. (INÉDITA/2023) De acordo com a Resolução CMN N. 4.893/2021, qual é o propósito da divulgação da política de segurança cibernética para os funcionários das instituições financeiras e para as empresas prestadoras de serviços a terceiros?
a) Assegurar que todos os funcionários e prestadores de serviços estejam cientes das penalidades por não cumprimento da política.
b) Promover a conscientização e garantir que a política seja implementada de forma eficaz, usando linguagem clara e acessível.
c) Oferecer treinamento detalhado em segurança cibernética a todos os funcionários e prestadores de serviços.
d) Divulgar os detalhes técnicos da política de segurança cibernética a todos os funcionários e prestadores de serviços.

a) Errada. A resolução não especifica a divulgação das penalidades como seu propósito principal.
b) Certa. A Resolução enfatiza a promoção da conscientização e eficácia na implementação da política (Art. 4º).
c) Errada. Embora o treinamento seja importante, a resolução não menciona a oferta de treinamento detalhado como parte da divulgação.
d) Errada. A resolução destaca a necessidade de linguagem clara e acessível, não necessariamente a divulgação de detalhes técnicos.
Letra b.

---

006. (INÉDITA/2023) Qual deve ser o conteúdo mínimo do plano de ação e resposta a incidentes estabelecido pelas instituições financeiras, segundo a Resolução CMN N. 4.893/2021?
a) Planos detalhados de recuperação de desastres e backups regulares de dados.
b) Ações para adequação à política de segurança cibernética, rotinas de prevenção e resposta a incidentes, e área responsável pelo controle dos efeitos de incidentes.
c) Estratégias para gerenciamento de mídias sociais e comunicação em caso de vazamento de dados.
d) Procedimentos para auditoria regular e avaliação de riscos cibernéticos.

a) Errada. Embora importantes, planos de recuperação de desastres e backups não são especificados como conteúdo mínimo na resolução.
b) Certa. A resolução especifica estas ações como conteúdo mínimo do plano de ação e resposta a incidentes (Art. 6º).
c) Errada. A resolução não menciona especificamente estratégias para gerenciamento de mídias sociais.
d) Errada. Procedimentos para auditoria e avaliação de riscos são importantes, mas não são citados como conteúdo mínimo na resolução.
Letra b.

---

007. (INÉDITA/2023) Conforme a Resolução CMN N. 4.893/2021, quais aspectos devem ser considerados pelas instituições financeiras ao contratar serviços de processamento e armazenamento de dados e de computação em nuvem?
a) Apenas o custo e a eficiência dos serviços de processamento e armazenamento de dados.
b) A conformidade com a legislação, a integridade dos dados, e a capacidade de auditoria do prestador de serviço.
c) A localização geográfica dos servidores e a popularidade do provedor de serviços de nuvem.
d) O impacto ambiental dos data centers e a política de responsabilidade social do prestador de serviço.

a) Errada. A resolução exige mais do que apenas considerar custo e eficiência.
b) Certa. A resolução enfatiza a conformidade legal, integridade de dados, e a capacidade de auditoria (Art. 12).
c) Errada. Localização geográfica e popularidade do provedor não são os principais critérios mencionados.
d) Errada. Impacto ambiental e responsabilidade social não são citados especificamente na resolução.
Letra b.

---

008. (INÉDITA/2023) De acordo com o Art. 12 da Resolução CMN N. 4.893/2021, quais são os procedimentos prévios necessários antes da contratação de serviços de computação em nuvem por instituições financeiras?
a) Avaliação da reputação do prestador de serviços e comparação de preços no mercado.
b) Análise da capacidade do prestador de serviço em assegurar a segurança e recuperação dos dados, e verificação da aderência a certificações exigidas.

c) Consulta pública para opiniões de consumidores e análise de tendências de mercado.
d) Verificação de antecedentes criminais dos diretores do prestador de serviço e análise de balanço financeiro da empresa.

a) Errada. Reputação e comparação de preços são importantes, mas não são os únicos aspectos mencionados na resolução.
b) Certa. A resolução destaca a importância da segurança e recuperação de dados e a aderência a certificações (Art. 12).
c) Errada. Consulta pública e análise de tendências de mercado não são procedimentos especificados na resolução.
d) Errada. A verificação de antecedentes criminais e análise financeira não são mencionadas na resolução.
Letra b.

---

009. (INÉDITA/2023) Qual é o procedimento exigido pela Resolução CMN N. 4.893/2021 em relação à comunicação com o Banco Central do Brasil após a contratação de serviços de computação em nuvem por instituições financeiras?
a) Não há necessidade de comunicação com o Banco Central do Brasil.
b) Comunicar ao Banco Central do Brasil dentro de dez dias após a contratação, incluindo informações sobre a empresa contratada, os serviços contratados, e a localização dos dados.
c) Apresentar um relatório anual detalhado ao Banco Central do Brasil sobre todos os serviços contratados.
d) Informar ao Banco Central do Brasil apenas no caso de contratação de serviços internacionais.

a) Errada. A resolução exige comunicação com o Banco Central do Brasil.
b) Certa. A comunicação deve incluir detalhes específicos e ser feita dentro de dez dias (Art. 15).
c) Errada. Não é mencionado um relatório anual, mas sim uma comunicação específica após cada contratação.
d) Errada. A comunicação é necessária independentemente de ser um serviço nacional ou internacional.
Letra b.

---

010. (INÉDITA/2023) De acordo com a Resolução CMN N. 4.893/2021, quais são as responsabilidades das instituições financeiras ao contratar serviços de computação em nuvem?

a) Garantir apenas o cumprimento da legislação e regulamentação em vigor.
b) Focar exclusivamente na eficiência operacional e na redução de custos.
c) Assegurar a confiabilidade, integridade, disponibilidade, segurança e sigilo dos serviços, além do cumprimento da legislação e regulamentação.
d) Delegar todas as responsabilidades ao prestador de serviço de computação em nuvem.

a) Errada. O cumprimento da legislação e regulamentação é necessário, mas não é a única responsabilidade.
b) Errada. Eficiência operacional e redução de custos são importantes, mas não são as únicas responsabilidades.
c) Certa. A resolução estabelece essas responsabilidades para as instituições financeiras (Art. 14).
d) Errada. As instituições não podem delegar todas as responsabilidades ao prestador de serviço.
Letra c.

---

011. (INÉDITA/2023) Quais são os requisitos estabelecidos pela Resolução CMN N. 4.893/2021 para a contratação de serviços de processamento, armazenamento de dados e computação em nuvem prestados no exterior por instituições financeiras?
a) Contratar apenas serviços localizados em países com acordos comerciais preferenciais com o Brasil.
b) Assegurar convênio para troca de informações, não prejudicar o funcionamento da instituição, definir locais específicos para prestação de serviços e prever alternativas de continuidade dos negócios.
c) Focar exclusivamente em serviços oferecidos por empresas multinacionais reconhecidas.
d) Garantir que os serviços sejam prestados unicamente em países com sistemas financeiros similares ao do Brasil.

a) Errada. A resolução não se limita a países com acordos comerciais preferenciais.
b) Certa. Reflete os requisitos estabelecidos no Art. 16.
c) Errada. Não se limita a empresas multinacionais, mas sim aos critérios estabelecidos na resolução.
d) Errada. Não é necessário que os países tenham sistemas financeiros similares ao do Brasil.
Letra b.

---

012. (INÉDITA/2023) Em caso de inexistência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras do país onde os serviços de computação em nuvem serão prestados, qual procedimento deve ser seguido, segundo a Resolução CMN N. 4.893/2021?

a) A instituição financeira deve imediatamente interromper a contratação do serviço.

b) Deve ser solicitada autorização do Banco Central do Brasil com antecedência mínima de sessenta dias da contratação ou alteração contratual.

c) A instituição financeira deve estabelecer seu próprio convênio com as autoridades locais.

d) É necessário realizar uma consulta pública antes de prosseguir com a contratação.

a) Errada. Não é necessário interromper imediatamente a contratação.

b) Certa. Conforme o Art. 16, § 1º, é necessário solicitar autorização com antecedência.

c) Errada. A instituição financeira não precisa estabelecer seu próprio convênio.

d) Errada. Não é mencionada a realização de consulta pública.

Letra b.

---

013. (INÉDITA/2023) De acordo com a Resolução CMN N. 4.893/2021, o que deve ser especificado nos contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem?

a) A localização exata dos servidores e a lista completa de clientes da empresa contratada.

b) Apenas a duração do contrato e os termos financeiros.

c) A indicação dos países e regiões onde os serviços serão prestados e os dados armazenados, processados e gerenciados.

d) Exclusivamente as medidas de segurança cibernética adotadas pela empresa contratada.

a) Errada. A resolução não exige a localização exata dos servidores ou a lista de clientes.

b) Errada. O contrato deve incluir mais do que apenas duração e termos financeiros.

c) Certa. Conforme Art. 17, I, é necessário especificar os locais de prestação de serviços e armazenamento de dados.

d) Errada. Embora as medidas de segurança sejam importantes, não são o único elemento a ser especificado.

Letra c.

---

014. (INÉDITA/2023) Segundo a Resolução CMN N. 4.893/2021, qual deve ser a ação da empresa contratada em caso de extinção do contrato de serviços de computação em nuvem?

a) Manter os dados armazenados indefinidamente.
b) Transferir os dados ao novo prestador de serviços ou à instituição contratante e depois excluí-los.
c) Vender os dados para terceiros como ativos da empresa.
d) Arquivar os dados em um sistema de armazenamento externo.

a) Errada. A resolução não permite a retenção indefinida dos dados.
b) Certa. Conforme Art. 17, IV, exige-se a transferência e posterior exclusão dos dados.
c) Errada. A venda de dados para terceiros é proibida pela resolução.
d) Errada. Arquivamento externo não é mencionado na resolução.
Letra b.

---

015. (INÉDITA/2023) O que está estipulado na Resolução CMN N. 4.893/2021 sobre o acesso do Banco Central do Brasil a informações relacionadas a serviços de computação em nuvem contratados por instituições financeiras?
a) O Banco Central do Brasil não tem permissão para acessar essas informações.
b) Acesso restrito apenas aos dados financeiros da instituição contratante.
c) Permissão para acessar contratos, documentações, dados armazenados e códigos de acesso.
d) Acesso somente em casos de investigações financeiras.

a) Errada. A resolução especifica que o Banco Central tem permissão de acesso.
b) Errada. O acesso não se limita apenas aos dados financeiros.
c) Certa. Conforme Art. 17, VII, o acesso abrange uma ampla gama de informações.
d) Errada. O acesso não se restringe a investigações financeiras.
Letra c.

---

016. (INÉDITA/2023) Quais serviços estão isentos das obrigações estipuladas nos artigos 11 a 17 da Resolução CMN N. 4.893/2021?
a) Serviços de telecomunicações e serviços de internet.
b) Sistemas operados por câmaras, prestadores de serviços de compensação e liquidação, ou entidades de registro ou depósito centralizado.
c) Todos os serviços de consultoria financeira.
d) Serviços de segurança física e vigilância.

a) Errada. Serviços de telecomunicações e de internet não estão especificamente isentos.
b) Certa. Conforme Art. 18, esses sistemas específicos estão isentos.

c) Errada. A resolução não isenta todos os serviços de consultoria financeira.
d) Errada. Serviços de segurança física e vigilância não são mencionados como isentos.
Letra b.

---

017. (INÉDITA/2023) Conforme a Resolução CMN N. 4.893/2021, quais aspectos devem ser abordados nas políticas de gerenciamento de riscos das instituições financeiras em relação à continuidade dos negócios?
a) Tratamento de incidentes cibernéticos, procedimentos para interrupção de serviços de TI e cenários para testes de continuidade de negócios.
b) Políticas de investimento e estratégias de marketing digital.
c) Estratégias de recrutamento de pessoal e políticas de remuneração.
d) Planos de expansão internacional e parcerias com outras instituições financeiras.

a) Certa. Reflete os elementos mencionados no Art. 19, incluindo tratamento de incidentes cibernéticos e procedimentos para interrupções de serviços.
b) Errada. Investimentos e estratégias de marketing digital não são mencionados no contexto de gerenciamento de riscos para continuidade de negócios.
c) Errada. Recrutamento e políticas de remuneração não são abordados neste contexto.
d) Errada. Planos de expansão internacional e parcerias não são mencionados no contexto de continuidade de negócios.
Letra a.

---

018. (INÉDITA/2023) De acordo com a Resolução CMN N. 4.893/2021, qual é o procedimento exigido das instituições financeiras em caso de incidentes relevantes ou interrupção de serviços de computação em nuvem?
a) Comunicação imediata ao Banco Central do Brasil e documentação detalhada das providências para o reinício das atividades.
b) Notificação apenas aos clientes afetados e manutenção de sigilo absoluto.
c) Comunicação exclusiva aos acionistas e investidores da instituição.
d) Suspensão imediata de todas as operações financeiras até resolução completa do incidente.

a) Certa. Conforme Art. 20, III, exige-se comunicação ao Banco Central e documentação das providências.
b) Errada. A comunicação não se limita aos clientes e não envolve manutenção de sigilo absoluto.

c) Errada. A comunicação deve ser feita ao Banco Central, não apenas aos acionistas e investidores.

d) Errada. A suspensão total das operações financeiras não é um procedimento exigido pela resolução.

Letra a.

Abra

caminhos

crie

futuros

gran.com.br