Estratégia Concursos

Aula 00 - Prof. Fernando Pedrosa

BANPARÁ - Passo Estratégico de Compliance e Governança Corporativa - 2024 (Pós-Edital)

Autor:
Alexandre Violato Peyerl, Fernando Pedrosa Lopes , Tulio Lages, Vinicius Rodrigues de Oliveira

06 de Novembro de 2024

RESOLUÇÃO CMN 4893

Sumário

Resolução CMN 4893 **1**

Conteúdo 1

ANÁLISE ESTATÍSTICA **1**

Glossário de termos 2

Roteiro de revisão 2

Conceitos Básicos 2

Capítulo I 3

Capítulo II 4

Capítulo III 12

Capítulo IV 21

Capítulo V 25

Aposta estratégica **28**

Questões Estratégicas 29

Questionário de revisão e aperfeiçoamento 30

Perguntas 31

Perguntas e Respostas 32

CONTEÚDO

Resolução CMN 4893. Capítulos I a V.

ANÁLISE ESTATÍSTICA

Devido ao baixo número de questões deste assunto, ainda não há dados estatísticos relevantes sobre a sua incidência em concursos anteriores.

GLOSSÁRIO DE TERMOS

Faremos uma lista de termos que são relevantes ao entendimento do assunto desta aula. Caso tenha alguma dúvida durante a leitura, esta seção pode lhe ajudar a esclarecer.

1. Resolução CMN 4.893: Regulamentação emitida pelo Conselho Monetário Nacional que estabelece diretrizes atualizadas para a política de segurança cibernética e os requisitos para contratação de serviços de processamento, armazenamento de dados e computação em nuvem por instituições financeiras.

2. Banco Central (BACEN): A autoridade monetária do Brasil, responsável por regular e supervisionar o sistema financeiro, garantindo sua estabilidade e conformidade com as leis e regulamentações vigentes.

3. Segurança Cibernética: Conjunto de tecnologias, processos e práticas projetadas para proteger redes, computadores, programas e dados de ataques, danos ou acessos não autorizados.

4. Computação em Nuvem: Modelo que permite acesso onipresente, conveniente e sob demanda a um conjunto compartilhado de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente provisionados e liberados com esforço mínimo de gestão ou interação com o provedor de serviço.

5. Trilhas de Auditoria: Registros detalhados de todas as ações, eventos ou atividades realizadas por usuários ou sistemas, essenciais para monitoramento, análise forense em caso de incidentes de segurança e auditorias.

6. Testes de Continuidade de Negócios: Avaliações e simulações realizadas para verificar a eficácia dos planos de continuidade de negócios, assegurando que a instituição possa continuar operando ou rapidamente retomar suas operações após interrupções significativas.

7. Certificações: Acreditações fornecidas por entidades reconhecidas que validam que um indivíduo ou empresa cumpre com certos padrões de qualidade e competência, particularmente em áreas técnicas e de segurança.

8. Governança Corporativa: Estruturas, práticas e processos utilizados para dirigir e gerir uma organização, garantindo a transparência, a responsabilidade e a segurança na condução de seus negócios.

9. Métricas e Indicadores: Ferramentas utilizadas para avaliar o desempenho, a eficiência e a eficácia de processos ou políticas, ajudando a monitorar a realização de objetivos e a identificar áreas que necessitam de melhorias.

10. Regime de Resolução: Procedimentos aplicados pelo Banco Central para intervir em uma instituição financeira que enfrenta problemas significativos de solvência ou liquidez, podendo incluir medidas como liquidação extrajudicial, intervenção ou administração especial temporária.

ROTEIRO DE REVISÃO

A ideia desta seção é apresentar um roteiro para que você realize uma revisão completa do assunto e, ao mesmo tempo, destacar aspectos do conteúdo que merecem atenção.

Conceitos Básicos

Resolução CMN no 4.893, de 26 de fevereiro de 2021

Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

O Banco Central do Brasil, na forma do art. 9o da Lei no 4.595, de 31 de dezembro de 1964, torna público que o Conselho Monetário Nacional, em sessão realizada em 25 de fevereiro de 2021, com base nos arts. 4o, inciso VIII, da referida Lei, 9o da Lei no 4.728, de 14 de julho de 1965, 7o e 23, alínea "a", da Lei no 6.099, de 12 de setembro de 1974, 1o, inciso II, da Lei no 10.194, de 14 de fevereiro de 2001, e 1o, § 1o, da Lei Complementar no 130, de 17 de abril de 2009, resolve:

A Resolução CMN 4.893, promulgada em 26 de fevereiro de 2021 pelo Banco Central do Brasil, estabelece diretrizes relativas à Política de Segurança Cibernética, além de definir critérios para

a contratação de serviços de processamento e armazenamento de dados e computação em nuvem, que devem ser seguidos pelas instituições reguladas pelo Banco Central. Esta matéria merece uma análise mais detalhada...

No contexto atual, fortemente influenciado pela globalização, a dependência em relação à tecnologia da informação é crescente. Com o avanço tecnológico, surgem também aumentos significativos nos riscos à segurança. Notavelmente durante a pandemia, observou-se um incremento nos ataques cibernéticos. A título de exemplo, a entidade na qual atuo sofreu recentemente um ataque de ransomware. Imagine agora a magnitude deste problema em ambientes de instituições financeiras...

Portanto, a referida resolução visa, especificamente, a dois propósitos fundamentais: (1) estabelecer diretrizes para uma política de segurança cibernética; e (2) estipular requisitos necessários à contratação de serviços de processamento e armazenamento de dados. Pode-se conjecturar sobre a vasta quantidade de dados sensíveis que uma instituição financeira possui. Consequentemente, é imprescindível a existência de uma política de segurança cibernética que oriente tais instituições quanto a possíveis incidentes e continuidade dos negócios.

Adicionalmente, é relevante mencionar que é prática comum entre as instituições financeiras a terceirização de serviços de processamento e armazenamento de dados, bem como de computação em nuvem. Muitas dessas instituições não possuem infraestrutura tecnológica adequada para manejar e armazenar tais volumes de dados, o que as leva a contratar esses serviços conforme a necessidade – o mesmo vale para a computação em nuvem.

Capítulo I

DO OBJETO E DO ÂMBITO DE APLICAÇÃO:

Art. 1o *Esta Resolução dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.*

Parágrafo único*. O disposto nesta Resolução não se aplica às instituições de pagamento, que devem observar a regulamentação emanada do Banco Central do Brasil, no exercício de suas atribuições legais.*

Neste artigo inicial, é essencial ressaltar que a resolução é aplicável exclusivamente às instituições autorizadas a operar pelo Banco Central do Brasil. Ela não se estende às instituições de pagamento, que disponibilizam serviços relacionados à compra, venda e movimentação de recursos financeiros destinados a pagamentos. Sua validade restringe-se unicamente às instituições financeiras, as quais fornecem serviços como empréstimos, financiamentos, investimentos, entre outros.

Capítulo II

Seção I

DA IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Art. 2o As instituições referidas no art. 1o 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.

§ 1o A política mencionada no caput deve ser compatível com:

I - o porte, o perfil de risco e o modelo de negócio da instituição;

II - a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e

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

As instituições financeiras habilitadas pelo Banco Central do Brasil devem estabelecer e preservar uma política de segurança cibernética fundamentada nos três pilares essenciais da segurança da informação: Confidencialidade, Integridade e Disponibilidade (CID). A violação de um ou mais desses princípios indica a ocorrência de um incidente de segurança da informação. Importante notar que, apesar de frequentemente ilustrados como uma pirâmide numerada, esses princípios não possuem uma ordem hierárquica.

De maneira concisa, a confidencialidade assegura que as informações não sejam acessíveis ou divulgadas a indivíduos, entidades ou processos não autorizados; a integridade protege a precisão e a completude dos ativos de informação; e a disponibilidade garante que as informações estejam acessíveis e utilizáveis conforme necessário por uma entidade autorizada.

A política de segurança cibernética deve alinhar-se com: (I) o tamanho, perfil de risco e modelo de negócio da instituição; (II) a natureza das operações e a complexidade dos produtos, serviços, atividades e processos envolvidos; e (III) a sensibilidade dos dados e informações sob a custódia da instituição. Portanto, não é adequado exigir a mesma política de segurança cibernética de uma grande instituição financeira e de uma de menor escala.

Esta compatibilidade deve ser aplicada também ao perfil de risco, modelo de negócio, natureza das operações, complexidade dos produtos/serviços e sensibilidade dos dados. As regras e procedimentos adotados devem ser nem excessivos nem insuficientes. Na prática, não é lógico que uma pequena instituição, que gerencia dados de baixa sensibilidade e realiza operações simples, seja submetida às mesmas exigências de segurança que um grande banco.

Assim, de maneira geral, quanto maior e mais complexa for a instituição financeira, maiores serão suas responsabilidades na implementação e manutenção de uma política de segurança adequada.

§ 2o Admite-se a adoção de política de segurança cibernética única por: I - conglomerado prudencial; e

II - sistema cooperativo de crédito.

§ 3o As instituições que não constituírem política de segurança cibernética própria em decorrência do disposto no § 2o devem formalizar a opção por essa faculdade em reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição.

Observa-se que é permitido às instituições financeiras implementarem uma política de segurança cibernética através de conglomerados prudenciais, que são grupos de instituições, ou sistemas cooperativos de crédito. Assim, instituições financeiras pertencentes ao mesmo grupo, como por exemplo o Banco do Brasil e a BB Consórcios, têm a possibilidade de adotar e seguir uma política única de segurança. É importante ressaltar que essa adoção necessita ser formalizada por meio do conselho de administração ou diretoria da respectiva instituição.

Art. 3o A política de segurança cibernética deve contemplar, no mínimo:

I - os objetivos de segurança cibernética da instituição;

II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética;

III - os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;

IV - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição;

V - As diretrizes para:

a) a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;

b) 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;

c) a classificação dos dados e das informações quanto à relevância; e

d) a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;

Este artigo delineia os requisitos fundamentais para a política de segurança cibernética, que incluem: objetivos; procedimentos e controles para minimizar vulnerabilidades a incidentes; controles específicos para garantir a rastreabilidade e a segurança de informações sensíveis; e o registro, a análise da causa/impacto, bem como o controle dos efeitos de incidentes significativos para as operações da instituição.

Adicionalmente, a política de segurança cibernética deve fornecer diretrizes para a criação de cenários de incidentes nos testes de continuidade de negócios. A continuidade de negócio refere-se aos procedimentos administrativos destinados a garantir a operação contínua de uma organização diante de uma indisponibilidade prolongada dos recursos essenciais para suas atividades. Por exemplo, caso ocorra um incêndio na sede do Banco do Brasil que destrua vários servidores do Centro de Processamento de Dados, o Plano de Continuidade de Negócio determinará as ações para manter as operações com o mínimo impacto possível para os usuários. Portanto, a política de segurança cibernética deve orientar a elaboração desses cenários.

A política também deve estabelecer diretrizes para a definição de procedimentos e controles focados na prevenção e no manejo de incidentes, a serem implementados por empresas terceirizadas que manuseiem dados ou informações sensíveis ou que sejam essenciais para as atividades operacionais da instituição. Muitas instituições financeiras optam pela terceirização de alguns serviços.

É preconizado que essas empresas prestadoras de serviços estabeleçam procedimentos e controles para prevenir e gerir potenciais incidentes relacionados a dados ou informações sensíveis ou essenciais para as operações. Cabe à instituição financeira a responsabilidade de definir esses procedimentos e controles.

A empresa contratada deve aderir às disposições estabelecidas na política de segurança cibernética da instituição contratante. Esta política também deve orientar a classificação dos dados e informações conforme sua relevância — não todas as informações possuem o mesmo nível de sensibilidade. Além disso, deve fornecer diretrizes para a determinação dos parâmetros usados na avaliação da relevância dos incidentes — nem todos os incidentes possuem o mesmo grau de gravidade.

VI - Os mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:

a) a implementação de programas de capacitação e de avaliação periódica de pessoal;

b) a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros; e

c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e

VII - As iniciativas para compartilhamento de informações sobre os incidentes relevantes, mencionados no inciso IV, com as demais instituições referidas no art. 1o.

§ 1o Na definição dos objetivos de segurança cibernética referidos no inciso I do caput, deve ser contemplada a capacidade da instituição para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

§ 2o Os procedimentos e os controles de que trata o inciso II do caput 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.

§ 3o Os procedimentos e os controles citados no inciso II do caput devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição.

§ 4o O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes, citados no inciso IV do caput, devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

§ 5o As diretrizes de que trata o inciso V, alínea "b", do caput, devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria instituição.

É essencial reconhecer que as instituições financeiras têm também a responsabilidade de promover a cultura de segurança cibernética. Um exemplo claro é quando uma pessoa, como uma avó, cai em um golpe e fornece sua senha bancária a um fraudador. As instituições

financeiras podem mitigar esses riscos disseminando uma cultura de segurança robusta. Isso pode ser alcançado através de programas de capacitação e avaliação de funcionários, educando clientes e usuários sobre medidas preventivas, e continuamente aprimorando seus procedimentos.

A política de segurança cibernética também deve incluir ações para o compartilhamento de informações sobre incidentes significativos com outras instituições financeiras. Tal prática é análoga à resposta a acidentes aéreos, onde os dados sobre um incidente contribuem para prevenir futuros acidentes em toda a indústria. Portanto, um incidente em uma instituição financeira pode ser visto como um problema em todo o sistema financeiro.

Além disso, os procedimentos e controles implementados para diminuir a vulnerabilidade da instituição a incidentes devem incluir:

a) Autenticação: métodos para verificar a identidade dos usuários ao acessar serviços financeiros;

b) Criptografia: estratégias para garantir que dados transmitidos mantenham sua confidencialidade, mesmo se interceptados;

c) Prevenção e detecção de intrusões: uso de ferramentas para identificar e alertar sobre possíveis invasores na rede da instituição financeira;

d) Prevenção de vazamentos de informações: medidas para evitar que dados sensíveis dos usuários sejam expostos externamente;

e) Testes periódicos e varreduras de vulnerabilidades: avaliações regulares para identificar possíveis falhas de segurança nos sistemas;

f) Proteção contra softwares maliciosos: defesas contra malwares, incluindo ransomware, que são ameaças cibernéticas frequentes;

g) Estabelecimento de mecanismos de rastreabilidade: criação de registros que permitam rastrear incidentes;

h) Controles de acesso e segmentação da rede: implementação de medidas para isolar e proteger dados críticos (Ex: VLAN);

i) Manutenção de cópias de segurança: estratégias para realizar backups de dados e informações de forma segura.

É crucial também destacar que os procedimentos e controles devem ser integrados desde a fase de desenvolvimento de software, garantindo a segurança desde a implementação das aplicações; o registro, análise de causa/impacto e controle dos efeitos de incidentes devem ser aplicados também às informações obtidas de prestadores de serviços terceirizados. Agora, discutiremos a divulgação da política de segurança cibernética.

Seção II

DA DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Art. 4o 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.

Art. 5o As instituições devem divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética.

É fundamental que a política de segurança cibernética, uma vez estabelecida, seja amplamente divulgada e disseminada entre os funcionários da instituição financeira e as empresas prestadoras de serviços. A própria instituição financeira precisa estar bem informada sobre a política para fomentar uma cultura organizacional de segurança, como discutido anteriormente; similarmente, as empresas contratadas precisam estar cientes da política para que possam prestar seus serviços de maneira apropriada.

Além disso, é imprescindível que a linguagem utilizada na comunicação da política seja clara, acessível e com um nível de detalhamento que seja adequado tanto às funções exercidas pelos colaboradores quanto à sensibilidade das informações manuseadas. Em uma instituição financeira, a diversidade de funcionários varia desde estagiários no início de sua carreira até especialistas em finanças, e inclui desde jovens nativos digitais até pessoas mais velhas, que podem ter diferentes níveis de familiaridade com a tecnologia.

Por essa razão, a política de segurança cibernética deve ser comunicada de forma a ser o mais clara e acessível possível, e o nível de detalhamento deve ser ajustado conforme a função desempenhada pelo colaborador e a sensibilidade das informações que ele maneja. Isso é crucial para minimizar os riscos de má interpretação. Por último, é recomendável que um resumo da política seja também divulgado ao público em geral, oferecendo uma visão geral das principais diretrizes.

Seção III

DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

Art. 6o As instituições referidas no art. 1o devem estabelecer plano de ação e de resposta a incidentes

visando à implementação da política de segurança cibernética.

Parágrafo único. O plano mencionado no caput deve abranger, no mínimo:

I - as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

II - as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e

III - a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

Art. 7o As instituições referidas no art. 1o devem designar diretor responsável pela política de

segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

Parágrafo único. O diretor mencionado no caput pode desempenhar outras funções na instituição, desde que não haja conflito de interesses.

Além da elaboração da política de segurança cibernética propriamente dita, é essencial que as instituições financeiras estabeleçam um plano de ação e resposta a incidentes para efetivar a aplicação dessa política. A importância deste plano reside não apenas na prevenção e no registro de incidentes, mas também na capacidade de implementar a política e gerenciar os incidentes efetivamente quando eles ocorrem. Esse plano deve incluir um conjunto mínimo de requisitos essenciais.

O plano de ação e resposta a incidentes deve conter: ações específicas que a instituição financeira necessita executar para alinhar suas estruturas organizacional e operacional com os princípios e diretrizes da política de segurança cibernética; rotinas, procedimentos, controles e tecnologias destinados à prevenção e ao gerenciamento de incidentes; e a definição clara da área encarregada de registrar e administrar os efeitos de incidentes significativos.

Por último, as instituições financeiras devem indicar um diretor responsável tanto pela política de segurança cibernética quanto pela gestão do plano de ação e resposta a incidentes. Não é problemático que este diretor acumule outras funções dentro da instituição, contanto que não exista conflito de interesses.

Art. 8o As instituições referidas no art. 1o devem elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, mencionado no art. 6o, com data-base de 31 de dezembro.

§ 1o O relatório de que trata o caput deve abordar, no mínimo:

I - a efetividade da implementação das ações descritas no art. 6o, parágrafo único, inciso I;

II - o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes descritos no art. 6o, parágrafo único, inciso II;

III - os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

IV - os resultados dos testes de continuidade de negócios, considerando cenários de

indisponibilidade ocasionada por incidentes.

§ 2o O relatório mencionado no caput deve ser:

I - submetido ao comitê de risco, quando existente; e

II - apresentado ao conselho de administração ou, na sua inexistência, à diretoria da instituição até

31 de março do ano seguinte ao da data-base.

Art. 9o A política de segurança cibernética referida no art. 2o e o plano de ação e de resposta a incidentes mencionado no art. 6o devem ser aprovados pelo conselho de administração ou, na sua inexistência, pela diretoria da instituição.

Art. 10. A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo, anualmente.

As instituições financeiras são obrigadas a elaborar um relatório anual que detalhe a implementação do plano de ação e resposta a incidentes, incluindo diversos aspectos críticos:

1. A eficácia das ações implementadas;

2. Um resumo dos resultados alcançados com a implementação;

3. Os incidentes significativos que ocorreram durante o ano;

4. Os resultados obtidos nos testes de continuidade de negócios.

Este relatório anual deve ser submetido ao comitê de risco, se houver, e apresentado ao conselho de administração ou, na ausência deste, à diretoria da instituição até o dia 31 de março do ano subsequente à data-base (31 de dezembro). A política de segurança cibernética e o plano de ação devem ser aprovados pelo conselho de administração, ou, na sua ausência, pela diretoria da instituição; esses documentos também devem ser formalmente documentados e revisados anualmente, no mínimo.

Dado o dinamismo do universo tecnológico, onde fraudes, golpes, malwares, vulnerabilidades, riscos e ataques emergem constantemente, é imperativo que a política de segurança cibernética e o plano de ação das instituições sejam documentados e revisados pelo menos uma vez ao ano. É crucial lembrar que o que está em jogo não são apenas instituições individuais, mas o sistema financeiro como um todo.

Capítulo III

Da Contratação De Serviços De Processamento E Armazenamento De Dados E De Computação Em Nuvem

Art. 11. As instituições referidas no art. 1o 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.

Art. 12. As instituições mencionadas no art. 1o, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, devem 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: a) o cumprimento da legislação e da regulamentação em vigor;

b) o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

e) 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;

f) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e

h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

§ 1o Na avaliação da relevância do serviço a ser contratado, mencionada no inciso I do caput, 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 realizada nos termos do art. 3o, inciso V, alínea "c".

§ 2o Os procedimentos de que trata o caput, inclusive as informações relativas à verificação mencionada no inciso II, devem ser documentados.

§ 3o No caso da execução de aplicativos por meio da internet, referidos no inciso III do art. 13, a instituição deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

§ 4o A instituição deve possuir recursos e competências necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso de recursos providos nos termos da alínea "f" do inciso II do caput.

As instituições financeiras têm a responsabilidade de garantir que suas políticas, estratégias e estruturas de gerenciamento de riscos, conforme estabelecido pelas normas regulatórias vigentes, incluam a contratação de serviços essenciais de processamento e armazenamento de dados e computação em nuvem, tanto nacional quanto internacionalmente. Isso se deve ao fato de que, atualmente, é comum que tais serviços sejam prestados por empresas terceirizadas.

Antes de efetuar a contratação desses serviços, as instituições financeiras devem implementar procedimentos alinhados a práticas de governança corporativa e gestão de riscos proporcionais à relevância do serviço e aos riscos envolvidos. Além disso, devem estabelecer procedimentos documentados que permitam avaliar a capacidade do fornecedor potencial em diversas áreas:

1. Cumprimento Regulatório: A empresa contratada deve ser capaz de cumprir com todas as leis e regulamentos aplicáveis.

2. Acesso e Recuperação de Dados: Deve garantir o acesso contínuo da instituição aos dados e assegurar a confidencialidade, integridade, disponibilidade e recuperação das informações processadas ou armazenadas.

3. Adesão a Certificações: A empresa deve atender às certificações exigidas pela instituição contratante.

4. Transparência e Monitoramento: Deve fornecer acesso a relatórios de auditoria independente, demonstrando a adequação dos procedimentos e controles utilizados.

5. Gestão de Informações e Dados do Cliente: A empresa deve prover recursos de gestão adequados, garantir a segregação dos dados dos clientes e assegurar a qualidade dos controles de acesso.

A instituição financeira deve monitorar rigorosamente se o prestador de serviços atende a todos esses requisitos. Além disso, ao avaliar a relevância do serviço contratado, deve considerar a criticidade e a sensibilidade dos dados e informações que serão processados, armazenados e gerenciados, levando em consideração a classificação de segurança cibernética.

Quando aplicativos forem operados via internet, a instituição deve assegurar que o prestador de serviços implemente controles robustos, como testes de regressão, para mitigar riscos associados à liberação de novas versões do aplicativo. Por fim, a instituição deve possuir as competências e recursos necessários para gerenciar adequadamente os serviços contratados, incluindo a capacidade de analisar informações e utilizar recursos de forma eficaz.

Art. 13. Para os fins do disposto nesta Resolução, 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:

I - 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;

II - implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

III - 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.

Art. 14. A instituição contratante dos serviços mencionados no art. 12 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 importância de estabelecer regras específicas para a contratação de serviços de computação em nuvem por instituições financeiras é ressaltada pelo contexto histórico e tecnológico que

moldou o cenário atual. Tradicionalmente, antes da popularização da internet banda larga e dos avanços tecnológicos associados, os bancos e outras instituições financeiras mantinham os dados dos clientes e transações armazenados internamente em seus próprios servidores, no modelo conhecido como On Premises. Este formato permitia um controle direto e relativamente simples sobre o acesso a dados pessoais, sensíveis e sigilosos.

No entanto, com o aumento da velocidade de internet, emergiu um modelo de negócios completamente novo: a computação em nuvem. Este modelo permite que o armazenamento e o processamento de dados sejam realizados em servidores de terceiros, oferecendo vantagens significativas como a redução de custos com infraestrutura, a otimização da capacidade computacional e a transferência de riscos e responsabilidades de manutenção para o prestador de serviços. Empresas como a Amazon AWS exemplificam o sucesso desse modelo, prestando serviços a uma vasta gama de clientes, incluindo grandes plataformas educacionais como o Estratégia Concursos.

A transição para a computação em nuvem, apesar de suas vantagens, apresenta desafios únicos, especialmente para instituições financeiras que lidam com dados extremamente sensíveis e estão sujeitas a rigorosas regulamentações de segurança e privacidade. A resolução em discussão foi desenvolvida em resposta à necessidade de assegurar que mesmo quando os dados são processados ou armazenados fora das instalações da instituição, em muitos casos por empresas estrangeiras, eles ainda devem ser gerenciados de acordo com os altos padrões exigidos pelo Banco Central e pelo Conselho Monetário Nacional.

As diretrizes estabelecidas na resolução especificam que os serviços de computação em nuvem devem fornecer, no mínimo:

- Recursos de processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais para que a instituição contratante possa implantar ou executar softwares, incluindo sistemas operacionais e aplicativos.
- A possibilidade de implantar ou executar aplicativos adquiridos ou desenvolvidos pela instituição contratante, usando os recursos computacionais do prestador de serviços.
- A execução, através da internet, de aplicativos desenvolvidos ou implantados pelo prestador de serviços, utilizando seus próprios recursos computacionais.

Ademais, a resolução enfatiza que a instituição contratante é responsável pela confiabilidade, integridade, disponibilidade, segurança e sigilo dos serviços contratados, assim como pelo cumprimento das leis e regulamentações aplicáveis. Isso sublinha que, em caso de incidentes, a responsabilidade final recai sobre a instituição financeira contratante, e não sobre o prestador do serviço. Essas medidas são vitais para garantir a proteção e a segurança dos dados financeiros sensíveis num ambiente cada vez mais globalizado e interconectado.

Art. 15. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pelas instituições referidas no art. 1o ao Banco Central do Brasil.

§ 1o A comunicação mencionada no caput deve conter as seguintes informações: I - a denominação da empresa contratada;

II - os serviços relevantes contratados; e

III - 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, definida nos termos do inciso III do art. 16, no caso de contratação no exterior.

§ 2o A comunicação de que trata o caput deve ser realizada até dez dias após a contratação dos serviços.

§ 3o As alterações contratuais que impliquem modificação das informações de que trata o § 1o devem ser comunicadas ao Banco Central do Brasil até dez dias após a alteração contratual.

A obrigatoriedade de comunicação por parte das instituições financeiras sobre a contratação de serviços de processamento, armazenamento de dados e de computação em nuvem é uma medida regulatória essencial para manter a transparência e a segurança das operações financeiras. Essa comunicação deve incluir detalhes como a denominação da empresa contratada, os serviços específicos que foram contratados, e a localização geográfica onde os dados serão armazenados, processados e gerenciados, especialmente quando se trata de contratações internacionais.

A exigência dessa comunicação tem uma razão fundamental: a legislação e as regulações sobre acesso a dados podem variar significativamente de um país para outro. Existem regiões que podem impor restrições ou mesmo proibir o acesso dos reguladores ou das próprias instituições financeiras aos dados armazenados. Isso pode criar situações complexas, por exemplo, onde o Banco Central do Brasil precisaria acessar informações para supervisão e não conseguisse devido a restrições locais.

Ao exigir que as instituições financeiras reportem esses detalhes ao Banco Central, o regulador busca assegurar que não haja impedimentos legais ou técnicos que comprometam a supervisão regulatória ou o controle sobre a gestão e segurança desses dados. Essa clareza também é crucial para garantir que as práticas de governança e risco dessas instituições estejam alinhadas com as expectativas e requisitos regulatórios.

Além disso, qualquer alteração contratual que modifique as informações inicialmente comunicadas, como mudanças nos locais de processamento ou nos serviços prestados, também deve ser reportada ao Banco Central em até 10 dias após a alteração. Isso é essencial para manter a atualização e a precisão das informações que o regulador possui, permitindo uma supervisão

efetiva e a tomada de decisões informadas em tempo real. Essas medidas são parte integrante dos esforços para manter o sistema financeiro seguro e estável, evitando surpresas que poderiam afetar negativamente a integridade e a operacionalidade das instituições financeiras.

Art. 16. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior deve observar os seguintes requisitos:

I - 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;

II - 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;

III - 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; e

IV - 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.

§ 1o No caso de inexistência de convênio nos termos do inciso I do caput, a instituição contratante deverá solicitar autorização do Banco Central do Brasil para:

I - a contratação do serviço, no prazo mínimo de sessenta dias antes da contratação, observado o disposto no art. 15, § 1o, desta Resolução; e

II - as alterações contratuais que impliquem modificação das informações de que trata o art. 15, § 1o, observando o prazo mínimo de sessenta dias antes da alteração contratual.

§ 2o Para atendimento aos incisos II e III do caput, 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.

§ 3o A comprovação do atendimento aos requisitos de que tratam os incisos I a IV do caput e o cumprimento da exigência de que trata o § 2o devem ser documentados.

a contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem realizada no exterior, as instituições financeiras brasileiras devem adotar precauções adicionais para assegurar a conformidade com as normas regulatórias e a integridade operacional. Essas precauções são especialmente necessárias para garantir que a prestação desses serviços não afete negativamente o funcionamento regular da instituição contratante nem interfira na supervisão exercida pelo Banco Central do Brasil (BACEN).

Etapas e Considerações para Contratação Internacional:

Verificação de Acordos de Troca de Informações: Antes de proceder com a contratação, a instituição financeira deve verificar se existe um convênio para troca de informações entre o BACEN e as autoridades supervisoras dos países onde os serviços serão prestados. Esse convênio é crucial para assegurar que o BACEN mantenha sua capacidade de supervisão efetiva sobre as atividades da instituição financeira, mesmo quando os dados são gerenciados fora do Brasil.

Solicitação de Autorização do BACEN: Caso não exista um acordo prévio entre o BACEN e as autoridades locais do país em questão, a instituição financeira deve solicitar uma autorização específica do BACEN. Essa autorização deve ser pedida com um prazo mínimo de 60 dias antes da formalização do contrato de serviço, proporcionando tempo suficiente para uma análise detalhada pela autoridade monetária.

Definição de Localidades e Alternativas de Continuidade: A instituição contratante deve definir previamente as regiões e países específicos onde os dados serão armazenados, processados e gerenciados. Além disso, deve prever alternativas para garantir a continuidade dos negócios em casos de impossibilidade de manutenção ou término do contrato de serviço.

Conformidade com Legislações Locais: As instituições financeiras devem verificar se a legislação e a regulamentação nos países escolhidos para a prestação dos serviços não impõem restrições que possam impedir o acesso aos dados pela instituição contratante ou pelo BACEN.

Documentação e Comprovação de Conformidade: É essencial que o cumprimento de todos esses requisitos, especialmente os detalhados no Art. 16 e a exigência do §2o, seja formalmente documentado. Essa documentação serve como prova de que todas as medidas regulatórias necessárias foram consideradas e implementadas.

Importância da Conformidade Regulatória:

Essas medidas são vitais para garantir que mesmo quando as instituições financeiras utilizam serviços de computação em nuvem e armazenamento de dados no exterior, elas continuem a operar dentro dos parâmetros de segurança e supervisão estabelecidos pelo BACEN. Elas também ajudam a mitigar riscos potenciais à estabilidade financeira da instituição e garantem a proteção dos dados dos clientes, que são frequentemente sensíveis e de natureza confidencial.

Art. 17. Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

I - 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;

II - a adoção de medidas de segurança para a transmissão e armazenamento dos dados citados no inciso I do caput;

III - a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;

IV - a obrigatoriedade, em caso de extinção do contrato, de:

a) transferência dos dados citados no inciso I do caput ao novo prestador de serviços ou à instituição

contratante; e

b) exclusão dos dados citados no inciso I do caput pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos;

V - o acesso da instituição contratante a:

a) informações fornecidas pela empresa contratada, visando a verificar o cumprimento do disposto

nos incisos I a III do caput;

b) informações relativas às certificações e aos relatórios de auditoria especializada, citados no art. 12, inciso II, alíneas "d" e "e"; e

c) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados, citados no art. 12, inciso II, alínea "f";

VI - a obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição;

VII - 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;

VIII - a adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e

IX - 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.

Parágrafo único. Os contratos mencionados no caput devem prever, para o caso da decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil:

I - 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 citados no inciso VII do caput que estejam em poder da empresa contratada; e

II - 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) 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; e

b) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

Art. 18. O disposto nos arts. 11 a 17 não se aplica 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.

A formulação de contratos para a prestação de serviços de processamento, armazenamento de dados e computação em nuvem deve ser meticulosa e prever diversas salvaguardas para proteger a instituição financeira contratante. Essas disposições contratuais são essenciais para assegurar não apenas a segurança dos dados, mas também a continuidade e a regularidade dos serviços, especialmente em situações críticas ou de mudança de fornecedor.

Disposições Importantes em Contratos de Serviço:

- Localização e Segurança dos Dados: Os contratos devem especificar claramente os países e as regiões onde os serviços serão prestados e os dados armazenados, processados e gerenciados. Deve-se incluir medidas de segurança rigorosas para a transmissão e armazenamento dos dados, bem como a manutenção da segregação dos dados e dos controles de acesso para proteger as informações dos clientes.
- Transferência e Exclusão de Dados: Em caso de extinção do contrato, é crucial prever a obrigatoriedade de transferir os dados para um novo prestador ou de volta para a instituição contratante, seguida pela exclusão completa dos dados pelo prestador de serviço substituído, após a confirmação de que a integridade e a disponibilidade dos dados transferidos foram verificadas.
- Acesso a Informações e Cumprimento Contratual: Os contratos devem garantir o acesso da instituição contratante a informações fornecidas pelo prestador de serviços, incluindo dados sobre certificações, relatórios de auditoria e recursos de gestão adequados para monitorar a prestação dos serviços.
- Subcontratação de Serviços: A obrigação de a empresa contratada notificar a instituição financeira sobre a subcontratação de serviços relevantes, assegurando transparência e controle contínuo sobre quem está manuseando os dados.

- Acesso do Banco Central: Permitir o acesso do Banco Central aos contratos, acordos, documentação e informações referentes aos serviços prestados, backups, e códigos de acesso, é fundamental para a supervisão regulatória.
- Resposta a Regimes de Resolução: Os contratos devem prever procedimentos específicos para o caso de um Regime de Resolução ser decretado, garantindo que o responsável pelo regime tenha acesso irrestrito a todas as informações e documentos necessários para administrar a situação.

Notificação de Interrupção de Serviços: A empresa contratada deve notificar a instituição financeira com antecedência mínima de 30 dias sobre qualquer intenção de interromper os serviços, com a possibilidade de estender este prazo por mais 30 dias em caso de necessidade, mesmo em situações de inadimplência.

Essas cláusulas são projetadas para proteger as operações financeiras e a integridade dos dados dos clientes das instituições financeiras, assegurando a conformidade contínua com as leis e regulamentos, além de preparar tanto a instituição quanto o prestador de serviços para lidar adequadamente com qualquer transição ou crise.

Capítulo IV

DISPOSIÇÕES GERAIS

Art. 19. As instituições referidas no art. 1o devem assegurar que suas políticas para gerenciamento de riscos previstas na regulamentação em vigor disponham, no tocante à continuidade de negócios, sobre:

I - o tratamento dos incidentes relevantes relacionados com o ambiente cibernético de que trata o art. 3o, inciso IV;

II - 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; e

III - os cenários de incidentes considerados nos testes de continuidade de negócios de que trata o art. 3o, inciso V, alínea "a".

Para assegurar uma gestão eficaz do risco e a continuidade de negócios, as instituições financeiras precisam incorporar em suas políticas de gerenciamento de riscos disposições específicas sobre como lidar com incidentes no ambiente cibernético. Essas políticas são vitais para a resiliência operacional e para garantir que os serviços permaneçam contínuos e seguros, mesmo diante de interrupções potenciais.

Elementos Críticos na Política de Continuidade de Negócios:

- Tratamento de Incidentes Cibernéticos: Deve-se detalhar como os incidentes cibernéticos serão identificados, classificados, respondidos e recuperados. Isso inclui a definição de quem são os responsáveis pelas diversas tarefas e como as comunicações internas e externas serão gerenciadas durante um incidente.
- Procedimentos em Caso de Interrupção de Serviços: As políticas devem claramente descrever os passos a seguir no caso de uma interrupção do serviço. Isso inclui cenários em que o prestador de serviço atual seja incapaz de continuar suas operações, exigindo uma transição rápida e segura para outro prestador.
- Cenários de Substituição de Prestadores de Serviço: Deve haver um plano estruturado para a substituição de prestadores de serviço que inclua a seleção e qualificação de novos prestadores, além de procedimentos para a transferência segura de dados e capacidades operacionais sem comprometer a segurança ou a funcionalidade do serviço.
- Testes de Continuidade: A política deve incorporar a realização regular de testes de continuidade que simulem diferentes cenários de interrupção para verificar a eficácia das medidas e procedimentos estabelecidos. Esses testes ajudam a identificar vulnerabilidades na estratégia de continuidade e permitem a correção antes que um incidente real ocorra.

Importância da Previsão de Cenários:

Prever cenários possíveis de interrupção é crucial para garantir que, quando uma interrupção ocorrer, a instituição esteja preparada para agir rapidamente e restaurar os serviços com o mínimo de perturbação possível. Isso é especialmente importante em um setor como o financeiro, onde a confiança do cliente e a integridade do mercado são fundamentais. Ao considerar incidentes relevantes e estabelecer procedimentos detalhados para cada cenário possível, as instituições financeiras podem se precaver contra diversos tipos de interrupções e assegurar que a transição para um novo prestador de serviços ocorra de maneira suave e segura, mantendo a operação normal para os usuários.

Art. 20. Os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à continuidade de negócios:

I - o tratamento previsto para mitigar os efeitos dos incidentes relevantes de que trata o inciso IV do art. 3o e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados;

II - o prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos, citados no inciso I do caput; e

III - a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes citados no inciso I do caput que

configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades.

Parágrafo único. As instituições devem estabelecer e documentar os critérios que configurem uma situação de crise de que trata o inciso III do caput.

Os procedimentos adotados pelas instituições financeiras para o gerenciamento de riscos e a continuidade dos negócios são cruciais para garantir a estabilidade e a confiança no sistema financeiro. Estes procedimentos devem ser meticulosamente planejados e implementados para abordar várias facetas de uma possível interrupção dos serviços.

Elementos Essenciais dos Procedimentos para Gerenciamento de Riscos:

- Mitigação dos Efeitos dos Incidentes: As políticas devem especificar as ações imediatas e de longo prazo para mitigar os efeitos de incidentes relevantes. Isso pode incluir medidas como a ativação de sistemas redundantes, o uso de backups para restaurar dados perdidos e a implementação de controles de segurança adicionais para prevenir futuros incidentes.
- Prazos para Normalização das Atividades: Deve ser estabelecido um cronograma claro para o reinício ou a normalização das atividades após uma interrupção. Este cronograma deve considerar a complexidade do sistema, a extensão do dano e os recursos disponíveis para recuperação.
- Comunicação com o Banco Central: A política deve incluir a obrigatoriedade de notificar o Banco Central de forma tempestiva sobre qualquer incidente ou interrupção que possa ser classificado como uma situação de crise. A notificação deve incluir detalhes sobre o incidente, as medidas tomadas para mitigar seus efeitos e o prazo estimado para a retomada normal das operações.

Definindo uma Situação de Crise:

Uma "situação de crise" é tipicamente definida como qualquer evento que possa ter um impacto severo na capacidade operacional da instituição financeira, na segurança dos ativos dos clientes ou na estabilidade do sistema financeiro como um todo. As próprias instituições financeiras são responsáveis por estabelecer e documentar os critérios específicos que definem uma situação de crise, levando em consideração:

- A natureza do incidente (por exemplo, ciberataque, falha física, erro humano).
- A extensão do impacto sobre as operações diárias.
- O potencial de dano à reputação da instituição.
- O risco de perda financeira significativa para a instituição ou seus clientes.
- O risco para a estabilidade do sistema financeiro.

Importância da Documentação:

A documentação desses critérios é fundamental não apenas para garantir uma resposta rápida e eficaz durante uma crise, mas também para fornecer transparência para o regulador e para os stakeholders da instituição. A clareza nos critérios também auxilia na preparação e no treinamento dos funcionários, assegurando que todos na organização compreendam suas responsabilidades durante uma situação de crise.

Ao estabelecer esses procedimentos e critérios, as instituições financeiras podem melhor gerenciar os riscos associados à continuidade dos negócios, minimizando as interrupções e mantendo a confiança dos clientes e dos mercados em sua capacidade de operar de forma segura e eficiente, mesmo diante de adversidades.

Art. 21. As instituições de que trata o art. 1o 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:

I - a definição de processos, testes e trilhas de auditoria; II - a definição de métricas e indicadores adequados; e

III - a identificação e a correção de eventuais deficiências.

§ 1o As notificações recebidas sobre a subcontratação de serviços relevantes descritas no art. 17, inciso VI, devem ser consideradas na definição dos mecanismos de que trata o caput.

§ 2o Os mecanismos de que trata o caput devem ser submetidos a testes periódicos pela auditoria interna, quando aplicável, compatíveis com os controles internos da instituição.

Para as instituições financeiras, é crucial estabelecer um sistema robusto de acompanhamento e controle para assegurar que a política de segurança cibernética, o plano de ação e resposta a incidentes, e os requisitos para a contratação de serviços sejam efetivamente implementados e mantenham sua eficácia ao longo do tempo. Isso envolve várias práticas e ferramentas de gestão de tecnologia da informação que facilitam a supervisão e a melhoria contínua dos processos de segurança.

Componentes chave para o acompanhamento e controle incluem:

- Definição de Processos: Estabelecer e documentar claramente todos os processos relacionados à segurança cibernética e à resposta a incidentes. Isso inclui desde o manejo inicial de um incidente até as estratégias de recuperação e de comunicação com partes interessadas.

- Realização de Testes: Implementar uma rotina de testes sistemáticos para avaliar a robustez das medidas de segurança e a prontidão da equipe frente a diferentes cenários de incidentes. Os testes podem incluir simulações de ataque, testes de penetração e exercícios de recuperação de desastres.
- Trilhas de Auditoria: Manter registros detalhados de todas as ações, eventos ou atividades realizadas pelos usuários ou sistemas. Estas trilhas são essenciais para o monitoramento, para a análise forense em caso de incidentes e para as auditorias regulatórias ou internas.
- Definição de Métricas e Indicadores: Utilizar métricas e indicadores de desempenho para monitorar a eficácia das políticas e dos procedimentos de segurança. Isso pode incluir indicadores como o tempo médio para detectar e responder a incidentes, a frequência de incidentes, e a eficácia das medidas de mitigação.
- Identificação e Correção de Deficiências: Através das trilhas de auditoria e das métricas, identificar e registrar quaisquer deficiências ou falhas nos processos de segurança. Estabelecer um método sistemático para a correção dessas deficiências, que pode incluir atualizações de software, mudanças nos procedimentos operacionais ou treinamentos adicionais para a equipe.

Importância da Gestão Continuada:

A implementação desses mecanismos de acompanhamento e controle não só ajuda a mitigar os riscos associados a segurança cibernética, mas também fortalece a cultura de segurança dentro da instituição financeira. Isso é fundamental para manter a confiança dos clientes e para cumprir com os requisitos regulatórios rigorosos do setor financeiro.

Adicionalmente, essas práticas permitem que a instituição se adapte rapidamente às mudanças tecnológicas e às novas ameaças emergentes no cenário digital, garantindo que as medidas de segurança estejam sempre atualizadas e sejam eficazes contra os riscos atuais e futuros.

Art. 22. Sem prejuízo do dever de sigilo e da livre concorrência, as instituições mencionadas no art. 1o devem desenvolver iniciativas para o compartilhamento de informações sobre os incidentes relevantes de que trata o art. 3o, inciso IV.

§ 1o O compartilhamento de que trata o caput deve abranger informações sobre incidentes relevantes recebidas de empresas prestadoras de serviços a terceiros.

§ 2o As informações compartilhadas devem estar disponíveis ao Banco Central do Brasil.

Como já dissemos anteriormente, incidentes afetam o sistema financeiro como um todo e, não apenas, instituições individuais. Logo, a resolução mostra mais uma vez sua preocupação com a disseminação de iniciativas para o compartilhamento de informações sobre incidentes relevantes

– sem prejuízo do dever de sigilo e da livre concorrência. As informações compartilhadas devem estar disponíveis ao Banco Central.

Capítulo V

DISPOSIÇÕES FINAIS

Art. 23. Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

I - o documento relativo à política de segurança cibernética, de que trata o art. 2o;

II - a ata de reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição, no caso de ser formalizada a opção de que trata o art. 2o, § 2o;

III - o documento relativo ao plano de ação e de resposta a incidentes, de que trata o art. 6o;

IV - o relatório anual, de que trata o art. 8o;

V - a documentação sobre os procedimentos de que trata o art. 12, § 2o;

VI - a documentação de que trata o art. 16, § 3o, no caso de serviços prestados no exterior;

VII - os contratos de que trata o art. 17, contado o prazo referido no caput a partir da extinção do contrato;

VIII - os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle de que trata o art. 21, contado o prazo referido no caput a partir da implementação dos citados mecanismos; e

IX - a documentação com os critérios que configurem uma situação de crise de que trata o art. 20, Parágrafo único.

Esse artigo traz uma lista de documentos que devem ficar à disposição do Banco Central pelo prazo de 5 anos. Em suma: documento de política de segurança cibernética; atas de reunião; documento do plano de ação e de resposta a incidentes; relatório anual; documentação sobre procedimentos; documentação de serviços prestados no exterior; contratos firmados; dados, registros e informações para acompanhamento e controle; e critérios para definição de situação de crise.

Art. 24. O Banco Central do Brasil poderá adotar as medidas necessárias para cumprimento do disposto nesta Resolução, bem como estabelecer:

I - os requisitos e os procedimentos para o compartilhamento de informações, nos termos do art. 22; II - a exigência de certificações e outros requisitos técnicos a serem requeridos das empresas

contratadas, pela instituição financeira contratante, na prestação dos serviços de que trata o art. 12;

III - os prazos máximos de que trata o art. 20, inciso II para reinício ou normalização das atividades ou dos serviços relevantes interrompidos; e

IV - os requisitos técnicos e procedimentos operacionais a serem observados pelas instituições para o cumprimento desta Resolução.

O Banco Central possui a prerrogativa de definir requisitos e procedimentos para a troca de informações; demandar certificações e demais requisitos técnicos das empresas contratadas; determinar prazos limites para a retomada ou regularização das atividades ou serviços relevantes que foram interrompidos; bem como estipular requisitos técnicos e procedimentos operacionais que as instituições devem seguir para atender a esta resolução.

É pertinente ressaltar neste artigo a importância atribuída por esta resolução à questão dos requisitos técnicos. Embora não seja mandatório que as instituições financeiras contratem empresas de grande porte, como a Amazon AWS, o Banco Central pode requerer que as empresas contratadas cumpram com certificações ou outros requisitos técnicos essenciais para assegurar sua aptidão em fornecer o serviço proposto.

Art. 25. As instituições referidas no art. 1o que, em 26 de abril de 2018, já tinham contratado a prestação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem devem adequar o contrato para a prestação de tais serviços:

I - ao cumprimento do disposto no art. 16, incisos I, II, IV e § 2o, no caso de serviços prestados no exterior; e

II - ao disposto nos arts. 15, § 1o, e 17.

Parágrafo único. O prazo previsto para adequação ao disposto no caput não pode ultrapassar 31 de

dezembro 2021.

Art. 26. 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 nesta Resolução, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação dos referidos serviços.

Art. 27. Ficam revogadas:

I - a Resolução no 4.658, de 26 de abril de 2018; e

II - a Resolução no 4.752, de 26 de setembro de 2019.

Art. 28. Esta Resolução entra em vigor em 1o de julho de 2021.

Esta resolução representa um avanço em relação às normativas anteriores. A Resolução CMN 4.658, datada de 26 de abril de 2018, foi modificada pela Resolução CMN 4.752, de 26 de setembro de 2019, e ambas foram subsequentemente revogadas com a promulgação da Resolução CMN 4.893, em 26 de fevereiro de 2021. Consequentemente, as instituições financeiras que já haviam contratado serviços abrangidos por esta resolução devem ajustar seus contratos até o dia 31 de dezembro de 2021.

Ademais, este artigo esclarece que o Banco Central poderá proibir ou impor restrições à contratação de serviços de processamento e armazenamento de dados e de computação em nuvem sempre que verificar a não conformidade com as diretrizes desta resolução, ou quando tais serviços limitarem a atuação do Banco Central do Brasil. Também será estabelecido um prazo para que as adequações necessárias sejam realizadas nos serviços mencionados.

APOSTA ESTRATÉGICA

A ideia desta seção é apresentar os pontos do conteúdo que mais possuem chances de serem cobrados em prova, considerando o histórico de questões da banca em provas de nível semelhante à nossa, bem como as inovações no conteúdo, na legislação e nos entendimentos doutrinários e jurisprudenciais[1].

Um aspecto fundamental da nossa aula que merece destaque é a importância do gerenciamento rigoroso da segurança cibernética nas instituições financeiras, conforme estabelecido pelas resoluções do Conselho Monetário Nacional (CMN). A evolução dessas resoluções, culminando na Resolução CMN 4.893 de 2021, demonstra um esforço contínuo e crescente para fortalecer as práticas de segurança cibernética em meio a um ambiente digital cada vez mais complexo e ameaçador. Esta resolução não só atualiza os padrões de segurança, mas também expande as exigências para a contratação de serviços de processamento e armazenamento de dados, e de computação em nuvem, garantindo que as instituições financeiras mantenham controles rigorosos e uma postura proativa na prevenção de incidentes cibernéticos. A implementação

[1] Vale deixar claro que nem sempre será possível realizar uma aposta estratégica para um determinado assunto, considerando que às vezes não é viável identificar os pontos mais prováveis de serem cobrados a partir de critérios objetivos ou minimamente razoáveis.

eficaz dessas políticas é vital para proteger as informações sensíveis dos clientes e manter a integridade do sistema financeiro.

Além disso, o papel do Banco Central na supervisão e no estabelecimento de prazos para a adequação dos serviços contratados é crucial. O Banco Central detém a autoridade para intervir, impondo restrições ou mesmo vetando a contratação de serviços externos que não cumpram as normativas estabelecidas. Isso sublinha a responsabilidade das instituições financeiras de não apenas escolher prestadores de serviços que atendam a rigorosos critérios técnicos e de segurança, mas também de assegurar uma transição e manutenção contínua desses padrões. A capacidade de resposta rápida e eficaz em caso de incidentes, e a comunicação transparente com as autoridades regulatórias, são componentes essenciais para a resiliência e a confiança no setor financeiro, fortalecendo o sistema contra vulnerabilidades cibernéticas em um mundo cada vez mais interconectado.

QUESTÕES ESTRATÉGICAS

Nesta seção, apresentamos e comentamos uma amostra de questões objetivas selecionadas estrategicamente: são questões com nível de dificuldade semelhante ao que você deve esperar para a sua prova e que, em conjunto, abordam os principais pontos do assunto.

A ideia, aqui, não é que você fixe o conteúdo por meio de uma bateria extensa de questões, mas que você faça uma boa revisão global do assunto a partir de, relativamente, poucas questões.

Este assunto ainda não tem um número significativo de questões.

1. **(CESGRANRIO / CEF – 2021)** A Resolução CMN n° 4.893, de 26 de fevereiro de 2021, dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Essa Resolução determina que a política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser, no mínimo, documentados e revisados:

a) trimestralmente

b) semestralmente

c) anualmente

d) bienalmente

e) trienalmente

Comentários:

De acordo com o Art. 10, a política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo, **anualmente**.

Gabarito: Letra C

---

2. (CFC / CFC – 2019) A Resolução CMN nº 4658, de 26/4/2018, estabeleceu normas sobre política de segurança cibernética e requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem que as instituições financeiras e demais instituições autorizadas a funcionar pelo BCB devem observar. Para tanto dispõe, entre outras exigências, que a aprovação da política de segurança cibernética deve ser realizada até 6 de maio de 2019, devendo contemplar alguns princípios. Sobre esse assunto, identifique os princípios abaixo e, em seguida, assinale a opção CORRETA.

I. Os objetivos de segurança cibernética da instituição.

II. Os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética.

III. Os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis.

IV. O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição.

Estão CERTOS os itens:

a) I, II, III e IV.

b) I, II e III, apenas.

c) I, III e IV, apenas.

d) II, III e IV, apenas.

Comentários:

(I) Correto, conforme Art. 3º, Inciso I; (II) Correto, conforme Art. 3º, Inciso II; (I) Correto, conforme Art. 3º, Inciso III; (I) Correto, conforme Art. 3º, Inciso IV.

Gabarito: Letra A

---

3. **(Inédita – Prof Fernando Pedrosa)** Quais são as consequências para uma instituição financeira se ela não cumprir os requisitos da Resolução CMN 4.893 de 2021?

   A) Pode receber uma multa simbólica
   B) Está sujeita à intervenção ou outras penalidades do Banco Central
   C) Não há consequências legais, apenas recomendações
   D) Recebe apenas uma advertência por escrito
   E) É obrigada a encerrar suas operações imediatamente

   Comentários: Se uma instituição financeira não cumprir os requisitos da Resolução CMN 4.893 de 2021, está sujeita à intervenção ou outras penalidades por parte do Banco Central, dependendo da gravidade da infração

   Gabarito: B

4. **(Inédita – Prof Fernando Pedrosa)** Qual o impacto de não existir um convênio de troca de informações entre o BACEN e as autoridades supervisoras do país onde serviços de computação em nuvem estão sendo contratados?

   A) A instituição pode prosseguir sem qualquer requisito adicional
   B) Não afeta a operação ou conformidade regulatória

C) A instituição deve interromper imediatamente todos os serviços contratados
D) A instituição deve solicitar uma autorização especial do BACEN
E) Apenas o fornecedor do serviço é afetado, sem impacto para a instituição

Comentários: Na ausência de um convênio de troca de informações, a instituição financeira precisa solicitar uma autorização especial do BACEN para garantir que ainda possa cumprir as normativas e supervisionar adequadamente a segurança e a gestão dos dados.

Gabarito: D

5. **(Inédita – Prof Fernando Pedrosa)** Quais procedimentos as instituições financeiras devem implementar de acordo com a Resolução CMN 4.893 para garantir a segurança cibernética?

A) Reduzir a frequência dos testes de penetração
B) Ignorar as trilhas de auditoria se não houver incidentes
C) Implementar medidas rigorosas de autenticação e criptografia
D) Confiar exclusivamente em tecnologias de firewall
E) Delegar a responsabilidade de segurança cibernética a terceiros

Comentários: Para garantir a segurança cibernética conforme a Resolução CMN 4.893, as instituições financeiras devem implementar medidas rigorosas como autenticação forte, criptografia de dados e outras práticas de segurança, além de realizar auditorias e monitoramento contínuo.

Gabarito: C

QUESTIONÁRIO DE REVISÃO E APERFEIÇOAMENTO

A ideia do questionário é elevar o nível da sua compreensão no assunto e, ao mesmo tempo, proporcionar uma outra forma de revisão de pontos importantes do conteúdo, a partir de perguntas que exigem respostas subjetivas.

São questões um pouco mais desafiadoras, porque a redação de seu enunciado não ajuda na sua resolução, como ocorre nas clássicas questões objetivas.

O objetivo é que você realize uma auto explicação mental de alguns pontos do conteúdo, para consolidar melhor o que aprendeu ;)

Além disso, as questões objetivas, em regra, abordam pontos isolados de um dado assunto. Assim, ao resolver várias questões objetivas, o candidato acaba memorizando pontos isolados do conteúdo, mas muitas vezes acaba não entendendo como esses pontos se conectam.

Assim, no questionário, buscaremos trazer também situações que ajudem você a conectar melhor os diversos pontos do conteúdo, na medida do possível.

É importante frisar que não estamos adentrando em um nível de profundidade maior que o exigido na sua prova, mas apenas permitindo que você compreenda melhor o assunto de modo a facilitar a resolução de questões objetivas típicas de concursos, ok?

Nosso compromisso é proporcionar a você uma revisão de alto nível!

Vamos ao nosso questionário:

Perguntas

1. Qual é o objetivo principal da Resolução CMN 4.893 de 2021?

2. Como as instituições financeiras devem proceder com contratos existentes sob as resoluções anteriores à Resolução CMN 4.893 de 2021?

3. Que papel o Banco Central desempenha em relação à supervisão das práticas de segurança cibernética das instituições financeiras?

4. Quais são as consequências para uma instituição financeira se ela não cumprir os requisitos da Resolução CMN 4.893 de 2021?

5. Como a Resolução CMN 4.893 de 2021 impacta a contratação de serviços no exterior por instituições financeiras?

6. Que medidas uma instituição financeira deve implementar para garantir a continuidade dos negócios conforme a Resolução CMN 4.893 de 2021?

7. Qual é a importância de manter trilhas de auditoria conforme discutido?

8. Como as métricas e indicadores são utilizados pelas instituições financeiras no contexto da Resolução CMN 4.893 de 2021?

9. Que tipo de testes as instituições financeiras devem realizar para garantir a segurança cibernética?

10. Qual a relevância de definir um prazo máximo para a normalização das atividades após uma interrupção, conforme a nova resolução?

11. Qual é o impacto de uma auditoria independente nas instituições financeiras conforme discutido?

12. Por que é essencial que as instituições financeiras mantenham a capacidade de substituir prestadores de serviços rapidamente?

13. Como o Banco Central utiliza as informações sobre a localização dos serviços contratados no exterior?

14. O que determina a exigência de notificação ao Banco Central em caso de interrupções ou incidentes?

15. Como as definições de uma "situação de crise" afetam a operação das instituições financeiras?

16. Qual é a importância das certificações exigidas pelo Banco Central para as empresas contratadas?

17. Como os testes de continuidade de negócios influenciam a resiliência das instituições financeiras?

18. Qual é o papel das trilhas de auditoria na manutenção da conformidade regulatória?

19. Por que é crucial definir prazos para a normalização das atividades após interrupções?

20. Como a exigência de notificação prévia de interrupções de serviços ao Banco Central beneficia o sistema financeiro?

Perguntas e Respostas

1. Qual é o objetivo principal da Resolução CMN 4.893 de 2021?

Resposta: O principal objetivo da Resolução CMN 4.893 de 2021 é atualizar e fortalecer as políticas de segurança cibernética nas instituições financeiras, estabelecendo requisitos rigorosos para a contratação de serviços de processamento, armazenamento de dados e computação em nuvem.

2. Como as instituições financeiras devem proceder com contratos existentes sob as resoluções anteriores à Resolução CMN 4.893 de 2021?

Resposta: As instituições financeiras devem ajustar seus contratos existentes para estar em conformidade com as novas diretrizes da Resolução CMN 4.893 de 2021 até o prazo final de 31 de dezembro de 2021.

3. Que papel o Banco Central desempenha em relação à supervisão das práticas de segurança cibernética das instituições financeiras?

Resposta: O Banco Central supervisiona e regula as práticas de segurança cibernética das instituições financeiras, podendo impor restrições e exigir ajustes nos serviços de processamento, armazenamento de dados e computação em nuvem para garantir conformidade com as resoluções pertinentes.

4. Quais são as consequências para uma instituição financeira se ela não cumprir os requisitos da Resolução CMN 4.893 de 2021?

Resposta: Se uma instituição financeira não cumprir os requisitos da Resolução CMN 4.893 de 2021, o Banco Central pode intervir, impondo restrições ou proibições à contratação de serviços que não estejam em conformidade, além de estabelecer prazos para a adequação necessária.

5. Como a Resolução CMN 4.893 de 2021 impacta a contratação de serviços no exterior por instituições financeiras?

Resposta: A resolução exige que as instituições financeiras comuniquem ao Banco Central os detalhes sobre a contratação de serviços no exterior, incluindo a localização dos dados e a conformidade com os regulamentos internacionais, para evitar limitações ao acesso dos dados pelo Banco Central.

6. Que medidas uma instituição financeira deve implementar para garantir a continuidade dos negócios conforme a Resolução CMN 4.893 de 2021?

Resposta: As instituições financeiras devem implementar planos de continuidade de negócios que incluam procedimentos para a mitigação de incidentes, prazos para a normalização das atividades após interrupções e estratégias para a substituição segura de prestadores de serviços.

7. Qual é a importância de manter trilhas de auditoria conforme discutido?

Resposta: As trilhas de auditoria são essenciais para monitorar todas as ações, eventos e atividades realizadas, permitindo análises forenses em caso de incidentes de segurança e auxiliando nas auditorias regulatórias ou internas.

8. Como as métricas e indicadores são utilizados pelas instituições financeiras no contexto da Resolução CMN 4.893 de 2021?

Resposta: Métricas e indicadores são usados para avaliar a eficácia das políticas e procedimentos de segurança, ajudando a identificar e corrigir deficiências, monitorar a resposta a incidentes e manter a conformidade regulatória.

9. Que tipo de testes as instituições financeiras devem realizar para garantir a segurança cibernética?

Resposta: As instituições financeiras devem realizar testes de penetração, simulações de ataque e exercícios de recuperação de desastres para avaliar a robustez de suas medidas de segurança e a prontidão de sua equipe para diferentes cenários de incidentes.

10. Qual a relevância de definir um prazo máximo para a normalização das atividades após uma interrupção, conforme a nova resolução?

Resposta: Definir um prazo máximo para a normalização das atividades após uma interrupção é crucial para minimizar o impacto operacional e financeiro de tais interrupções, garantindo que a instituição possa retomar suas operações de forma eficiente e segura.

11. Qual é o impacto de uma auditoria independente nas instituições financeiras conforme discutido?

Resposta: Uma auditoria independente ajuda a verificar a conformidade com os padrões e regulamentos estabelecidos, assegurando que as medidas de segurança cibernética e os processos operacionais das instituições financeiras sejam apropriados e eficazes.

12. Por que é essencial que as instituições financeiras mantenham a capacidade de substituir prestadores de serviços rapidamente?

Resposta: Manter a capacidade de substituir prestadores de serviços rapidamente é essencial para assegurar a continuidade dos negócios e mitigar riscos associados à dependência de um único fornecedor, especialmente em situações de falha ou interrupção do serviço.

13. Como o Banco Central utiliza as informações sobre a localização dos serviços contratados no exterior?

Resposta: O Banco Central utiliza essas informações para assegurar que não haja restrições regulatórias ou legais que impeçam o acesso aos dados necessários para a supervisão e controle das atividades financeiras, além de garantir a conformidade com normas internacionais.

14. O que determina a exigência de notificação ao Banco Central em caso de interrupções ou incidentes?

Resposta: A exigência de notificação ao Banco Central em caso de interrupções ou incidentes visa permitir uma resposta regulatória adequada e garantir que medidas apropriadas sejam tomadas para restaurar os serviços e proteger os consumidores.

15. Como as definições de uma "situação de crise" afetam a operação das instituições financeiras?

Resposta: As definições de uma "situação de crise" estabelecem um limiar para ativação de procedimentos especiais de gestão de risco e resposta a incidentes, influenciando como as instituições se preparam e respondem a eventos significativos.

16. Qual é a importância das certificações exigidas pelo Banco Central para as empresas contratadas?

Resposta: As certificações exigidas pelo Banco Central garantem que as empresas contratadas atendam a padrões mínimos de segurança e competência técnica, reduzindo o risco de falhas e exposição a vulnerabilidades cibernéticas.

17. Como os testes de continuidade de negócios influenciam a resiliência das instituições financeiras?

Resposta: Os testes de continuidade de negócios ajudam a identificar pontos fracos nos planos de resposta a incidentes e garantem que a instituição possa continuar operando eficazmente após um evento disruptivo, melhorando sua resiliência global.

18. Qual é o papel das trilhas de auditoria na manutenção da conformidade regulatória?

Resposta: As trilhas de auditoria fornecem um registro detalhado de todas as atividades, permitindo a verificação do cumprimento das políticas internas e regulamentos externos, além de auxiliar na detecção e análise de incidentes de segurança.

19. Por que é crucial definir prazos para a normalização das atividades após interrupções?

Resposta: Definir prazos para a normalização das atividades é crucial para minimizar o tempo de inatividade, reduzir o impacto financeiro e operacional de interrupções e assegurar que os serviços aos clientes sejam restaurados rapidamente e de maneira ordenada.

20. Como a exigência de notificação prévia de interrupções de serviços ao Banco Central beneficia o sistema financeiro?

Resposta: A exigência de notificação prévia permite que o Banco Central prepare respostas regulatórias e supervisione as medidas de mitigação e recuperação, garantindo uma gestão eficaz de crises e a estabilidade do sistema financeiro.

LISTA DE QUESTÕES ESTRATÉGICAS

1. **(CESGRANRIO / CEF – 2021)** A Resolução CMN n° 4.893, de 26 de fevereiro de 2021, dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Essa Resolução determina que a política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser, no mínimo, documentados e revisados:

a) trimestralmente

b) semestralmente

c) anualmente

d) bienalmente

e) trienalmente

2. **(CFC / CFC – 2019)** A Resolução CMN nº 4658, de 26/4/2018, estabeleceu normas sobre política de segurança cibernética e requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem que as instituições financeiras e demais instituições autorizadas a funcionar pelo BCB devem observar. Para tanto dispõe, entre outras exigências, que a aprovação da política de segurança cibernética deve ser realizada até 6 de maio de 2019, devendo contemplar alguns princípios. Sobre esse assunto, identifique os princípios abaixo e, em seguida, assinale a opção CORRETA.

I. Os objetivos de segurança cibernética da instituição.

II. Os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética.

III. Os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis.

IV. O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição.

Estão CERTOS os itens:

a) I, II, III e IV.

b) I, II e III, apenas.

c) I, III e IV, apenas.

d) II, III e IV, apenas.

3. **(Inédita – Prof Fernando Pedrosa)** Quais são as consequências para uma instituição financeira se ela não cumprir os requisitos da Resolução CMN 4.893 de 2021?

A) Pode receber uma multa simbólica
B) Está sujeita à intervenção ou outras penalidades do Banco Central
C) Não há consequências legais, apenas recomendações
D) Recebe apenas uma advertência por escrito
E) É obrigada a encerrar suas operações imediatamente

4. **(Inédita – Prof Fernando Pedrosa)** Qual o impacto de não existir um convênio de troca de informações entre o BACEN e as autoridades supervisoras do país onde serviços de computação em nuvem estão sendo contratados?

   A) A instituição pode prosseguir sem qualquer requisito adicional
   B) Não afeta a operação ou conformidade regulatória
   C) A instituição deve interromper imediatamente todos os serviços contratados
   D) A instituição deve solicitar uma autorização especial do BACEN
   E) Apenas o fornecedor do serviço é afetado, sem impacto para a instituição

5. **(Inédita – Prof Fernando Pedrosa)** Quais procedimentos as instituições financeiras devem implementar de acordo com a Resolução CMN 4.893 para garantir a segurança cibernética?

   A) Reduzir a frequência dos testes de penetração
   B) Ignorar as trilhas de auditoria se não houver incidentes
   C) Implementar medidas rigorosas de autenticação e criptografia
   D) Confiar exclusivamente em tecnologias de firewall
   E) Delegar a responsabilidade de segurança cibernética a terceiros

Gabaritos

1. C
2. A
3. B
4. D
5. C

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.