Aula 13 - Prof Celso Natale

Banco do Brasil - Conhecimentos Bancários - 2023 (Pós-Edital)

Autor:
Celso Natale, Equipe Legislação Específica Estratégia Concursos, Stefan Fantini

17 de Janeiro de 2023

SUMÁRIO

1 Resolução CMN nº 4.893/2021: Segurança Cibernética 3

1.1 Política de Segurança Cibernética 3

1.2 Plano de ação e de resposta a incidentes 5

1.3 Contratação de serviços de processamento e armazenamento de dados e de computação em nuvem 6

Questões Comentadas 10

Lista de Questões..... 21

Gabarito..... 26

INTRODUÇÃO

Saudações!

Nesta aula, veremos o seguinte normativo:

21 - Segurança cibernética: Resolução CMN nº 4.893, de 26/02/2021.

Então só vamos!!

@profcelsonatale

1 Resolução CMN nº 4.893/2021: Segurança Cibernética

A **Resolução nº 4.893**, de 26 de fevereiro de 2021, do Conselho Monetário Nacional (CMN), dispõe sobre:

1. a **política de segurança cibernética**; e
2. **requisitos para a contratação** de serviços de processamento e armazenamento de dados e de computação em nuvem...

... a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Sendo assim, ela trata especificamente sobre a **segurança de dados** no ambiente cibernético (algo como o "mundo virtual", o "digital").

Nesse ambiente, os dados circulam o tempo todo, com muita velocidade. Muitas vezes, os dados trafegam em servidores espalhados pelo mundo todo, ficam **armazenados** e são **processados** fora da instituição – o próprio conceito de *computação em nuvem*.

Iremos aprofundar alguns conceitos técnicos oportunamente, mas, por enquanto, avançaremos no primeiro tema da aula.

1.1 Política de Segurança Cibernética

Segundo a Resolução, as instituições devem implementar e manter **política de segurança cibernética**, ou seja, um conjunto de regras e procedimentos para lidar com os riscos à segurança dos dados no ambiente digital.

Essa a política deve assegurar, em relação aos dados:

- confidencialidade
- integridade
- disponibilidade

Como estamos falando de um conjunto de regras e procedimentos, é importante que eles não sejam nem excessivos, nem insuficientes.

Na prática, não é razoável que uma pequena instituição – que lide com dados pouco sensíveis e realize apenas operações simples – observe as mesmas regras de um grande banco.

Por isso, a política de 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.

Outra determinação bastante razoável na Resolução é a possibilidade de adoção de uma política única por conglomerado (grupos de instituições) ou sistema cooperativo.

Assim, instituições financeiras do mesmo grupo (como Banco do Brasil e BB Consórcios, por exemplo) podem implementar e seguir a mesma política.

A Resolução determina o mínimo que a política de segurança cibernética deve contemplar:

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, abrangendo, no mínimo:
    a) a autenticação
    b) a criptografia
    c) a prevenção e a detecção de intrusão
    d) a prevenção de vazamento de informações
    e) a realização periódica de testes e varreduras para detecção de vulnerabilidades
    f) a proteção contra softwares maliciosos
    g) o estabelecimento de mecanismos de rastreabilidade
    h) os controles de acesso e de segmentação da rede de computadores
    i) a manutenção de cópias de segurança dos dados e das informações
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, abrangendo informações recebidas de empresas prestadoras de serviços a terceiros.
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;
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.

E claro, de nada adiantaria escrever uma bela e complexa política, se ela não for de conhecimento e compreensão amplos dos funcionários e contratados pela instituição.

Por isso, a **política de segurança cibernética deve ser divulgada**, mediante **linguagem clara**, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.

Portanto, há diferentes níveis de detalhamento, pois nem todos os funcionários e contratados precisam ou mesmo detém a capacidade técnica para conhecer toda a política.

Assim, os envolvidos mais diretamente com os procedimentos devem conhecer detalhes, enquanto funcionário que apenas aplicação em menor nível, podem ter acesso a uma versão simplificada.

Na verdade, até mesmo **o público deve ter acesso a resumo** contendo as linhas gerais da política de segurança cibernética.

1.2 Plano de ação e de resposta a incidentes

Além da política, as instituições devem estabelecer **plano de ação e de resposta a incidentes** visando à implementação da política de segurança cibernética.

Afinal, tão importante quanto evitar e registrar os incidentes, é saber como aplicar a política e lidar com os problemas caso ocorram.

Esse 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;
III. a **área responsável** pelo registro e controle dos efeitos de incidentes relevantes.

As instituições devem elaborar **relatório anual** sobre a implementação do plano de ação e de resposta a incidentes, abordando, entre outras coisas:

- a efetividade da implementação das ações;
- o resumo dos resultados obtidos na implementação;

- os incidentes relevantes ocorridos
- os resultados dos testes de continuidade de negócios.

Agora preste bem atenção, pois os tópicos a seguir se aplicam tanto à Política quanto ao Plano.

As instituições devem designar **diretor responsável** pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes. Ele pode desempenhar outras funções na instituição, desde que, é claro, não haja conflito de interesses.

A política de segurança cibernética e o plano de ação devem:

- ser aprovados pelo conselho de administração ou, na sua inexistência, pela diretoria da instituição;
- **documentados e revisados**, no mínimo, anualmente;
- ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos.

Certo! Vamos falar sobre a contração de serviços.

1.3 Contratação de serviços de processamento e armazenamento de dados e de computação em nuvem

Para compreender por que foi importante, para o regulador, determinar regras específicas para a contratação desses serviços, precisamos entender como era antes dessas tecnologias.

Um banco (ou outra instituição), armazena dados dos clientes e de transações. Dados pessoais, sensíveis e sigilosos, que podem provocar grande estrago se caírem em mãos erradas.

Antes de avanços tecnológicos, principalmente a internet de conexão rápida (banda larga), esses dados ficavam armazenados em computadores da própria instituição: os bancos de dados e o processamento dos dados ocorria "dentro de casa".

Como os bancos de dados estavam dentro da própria instituição, controlar o acesso a esses dados era relativamente simples. É claro que os dados também trafegavam – entre a agência e a matriz, por exemplo –, mas isso também ocorria em redes internas e fechadas.

Não fazia sentido, do ponto de vista econômico, guardar os dados em outro lugar, muito menos usar capacidade de processamento de outras empresas. *Quem já baixou músicas no início dos anos 2000 sabe bem o motivo: eram horas para baixar um arquivo com 3 min de música.*

Contudo, com a ampliação da velocidade da internet, um novo modelo de negócios passou a fazer sentido: a **computação em nuvem**.

Empresas de tecnologia passaram a oferecer armazenamento de dados em seus próprios servidores. Quem contrata, não precisa se preocupar com esses bancos de dados. É só entrar na

conta e acessar os arquivos, que ficam em servidores externos à instituição, sem ela sequer precisar saber onde, exatamente: por isso, a expressão "na nuvem" pegou.

Além do armazenamento dos arquivos, o processamento de dados também é oferecido. Se uma instituição precisa de supercomputadores para processar volumes imensos de dados, ela não precisa comprar e fazer manutenção desses equipamentos: basta contratar uma empresa de tecnologia e pagar para usar esses processadores *(a Amazon é a maior do segmento, atualmente, e empresas do mundo todo contratam esses serviços. Aposto que você conhece muitas delas. Ou você achou que a riqueza do Jeff Bezos veio só de vender livros?)*

Mas chegando ao ponto que eu queria: dados sensíveis e sigilosos "dentro" de instituições financeiras é uma coisa; elas seguem uma série de regras do BCB e do CMN, os reguladores têm amplo acesso, e as conhecem bem.

Mas esses mesmos dados armazenados e processados em servidores espalhados pelo mundo, de propriedade de empresas que, na maioria das vezes, sequer são brasileiras, é outra coisa completamente diferente.

E daí vem uma parte específica da Resolução apenas para tratar disso.

Para começar, é definido de forma mais técnica o que significa computação em nuvem:

> *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, dos aplicativos*** *implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.*

Também é determinado que a **instituição contratante 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.

Quer dizer que não adianta colocar a culpa na contratada: a responsabilidade, perante as autoridades (CMN e BCB), é da instituição contratante.

Então, de acordo com a norma, as instituições devem assegurar que suas **políticas**, estratégias e estruturas para gerenciamento de riscos, 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.

Isso significa que a política deve prever procedimentos específicos para contratação desse tipo de serviço.

E mais: antes de contratar, 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.

Todos esses procedimentos devem ser **documentados**.

E após a contratação, em até 10 dias, essa contratação deve ser comunicada pelas instituições ao Banco Central do Brasil, bem como quaisquer alterações contratuais que impliquem modificação relevante.

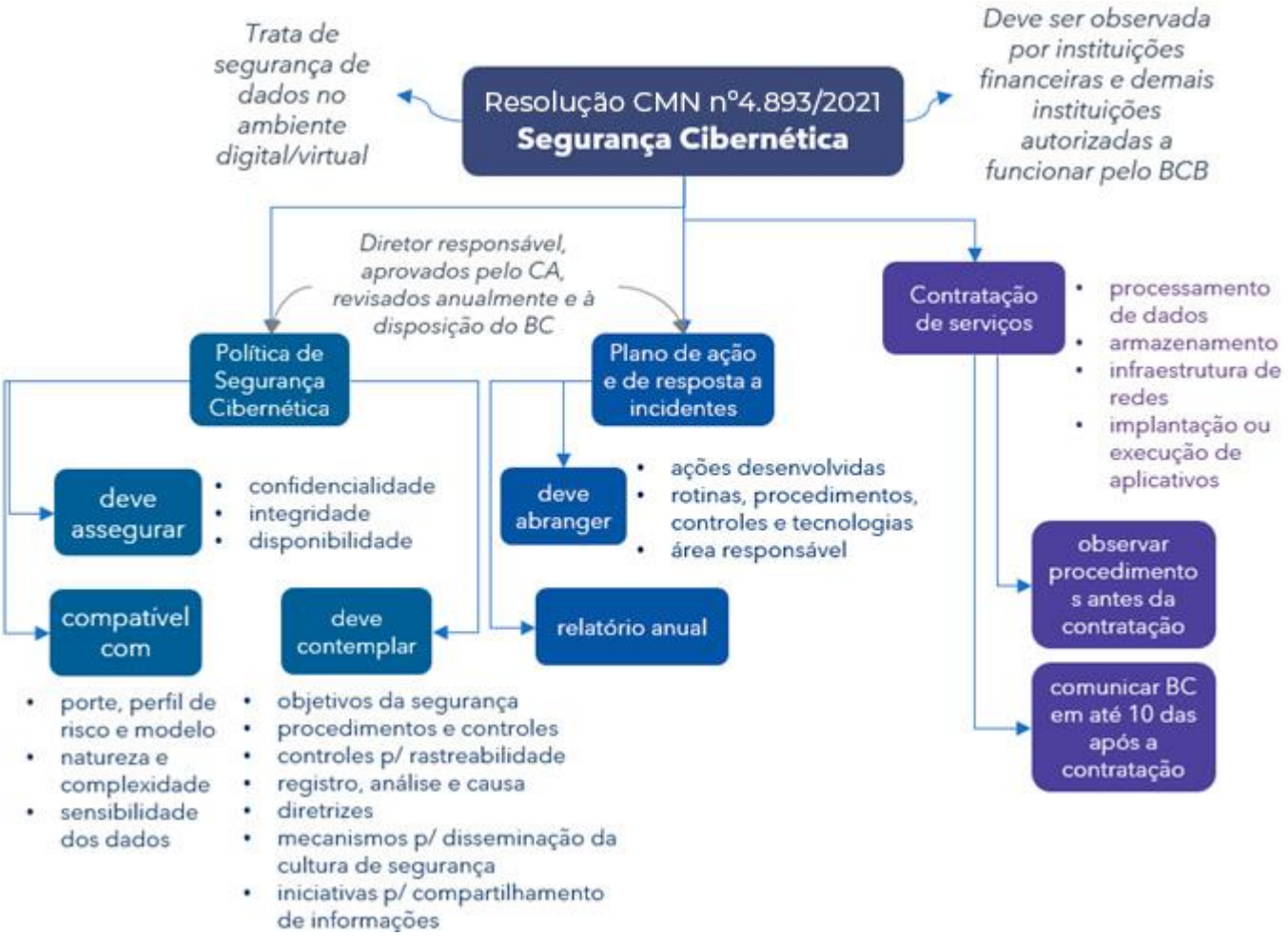
E por falar em **BCB**, além de ter acesso aos contratos, ele pode:

- **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;
    - 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 desta Resolução.

- 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 das normas, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação dos referidos serviços.

E é isso aí. Agora, só um bom resumo para fechar.



QUESTÕES COMENTADAS

1. (2019/CAE-CFC/Cadastro Nacional de Auditores Independentes BCB)

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:

> Antes de começarmos, um aviso: observe que essa questão menciona a Resolução CMN nº **4.658**/2018. Ela é a antecessora da Resolução nº **4.893**/2021, e tratava do mesmo tema, sendo idêntica na maioria dos pontos.
> Portanto, tive o cuidado de selecionar apenas questões que não entrem em conflito, ou seja, você pode resolver normalmente, como se a questão estivesse mencionando a Resolução nº 4.893/2021.

Todas estão corretas, então aproveitamos para revisar.

A Resolução determina o mínimo que a política de segurança cibernética deve contemplar:

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, abrangendo, no mínimo:
    a) a autenticação
    b) a criptografia
    c) a prevenção e a detecção de intrusão

d) a prevenção de vazamento de informações
e) a realização periódica de testes e varreduras para detecção de vulnerabilidades
f) a proteção contra softwares maliciosos
g) o estabelecimento de mecanismos de rastreabilidade
h) os controles de acesso e de segmentação da rede de computadores
i) a manutenção de cópias de segurança dos dados e das informações

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;
   a) 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.

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;

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.

Gabarito: "a"

2. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A política de segurança cibernética deve assegurar, em relação aos dados, EXCETO

a) disponibilidade.

b) integridade.

c) portabilidade.

d) segurança.
e) confidencialidade

Comentários:

Devemos marcar a alternativa errada, pois o comando da questão contém a expressão "exceto). Sendo assim, vimos que a política deve assegurar:

- confidencialidade (E)
- integridade (B)
- disponibilidade (A)

"Segurança" (D), é um termo que engloba todas as demais, dado o contexto da política.

Apenas "portabilidade" não é prevista na norma como algo a ser assegurado.

Gabarito: "c"

3. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

Sobre esse assunto, de acordo Resolução, a política de segurança 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. as políticas de segurança pública do município em que está localiza a agência ou filial

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

Estão CERTOS apenas 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.
e) I, II e IV, apenas

Comentários:

A política de 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.

Portanto, por mais razoável que seja supor que a política deve ser compatível com as regras de segurança pública municipais, a norma nada diz a esse respeito.

Gabarito: "e"

4. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A Resolução determina que a política de segurança cibernética deve contemplar os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética, abrangendo

a) a prevenção de compartilhamento de informações

b) a vedação à criptografia

c) a realização de varreduras posteriores à detecção de vulnerabilidades

d) a proteção contra cópias de segurança dos dados e das informações

e) o estabelecimento de mecanismos de rastreabilidade

Comentários:

Vamos lembrar!

A Resolução determina o mínimo que a política de segurança cibernética deve contemplar:

I. os **procedimentos e os controles** adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética, abrangendo, no mínimo:
   a) a autenticação
   b) a criptografia ("b" errada)
   c) a prevenção e a detecção de intrusão
   d) a prevenção de vazamento de informações ("a" errada. Compartilhamento não é vazamento)
   e) a realização periódica de testes e varreduras para detecção de vulnerabilidades ("c" errada. Os testes e varreduras são periódicos, e não após a detecção)
   f) a proteção contra softwares maliciosos
   g) o estabelecimento de mecanismos de rastreabilidade ("e" é o gabarito!)
   h) os controles de acesso e de segmentação da rede de computadores
   i) a manutenção de cópias de segurança dos dados e das informações ("d" errada)

Gabarito: "e"

5. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A divulgação da política de segurança deve

a) ser realizada sempre em linguagem técnica, adequada ao público especializado.

b) ter nível de detalhamento máximo, a todos os públicos.

c) ser vedada, por tratar de temas sensíveis.

d) ser realizada, de forma resumida, ao público.

e) ser restrita aos funcionários e contratados.

Comentários:

Vamos analisar as alternativas.

a) ser realizada sempre em linguagem técnica, adequada ao público especializado.

Errado. A linguagem deve ser clara e acessível.

b) ter nível de detalhamento máximo, a todos os públicos.

Errado. O nível de detalhamento deve ser compatível com as funções desempenhadas e com a sensibilidade das informações

c) ser vedada, por tratar de temas sensíveis.

Errado. A divulgação, como vimos, deve ocorrer, ainda que em diferentes graus.

d) ser realizada, de forma resumida, ao público.

Certo! O público deve ter acesso a resumo contendo as linhas gerais da política de segurança cibernética.

e) ser restrita aos funcionários e contratados.

Errada, pelo mesmo motivo que torna "d" o gabarito.

Gabarito: "d"

6. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A respeito do plano de ação e de resposta a incidentes, a norma determina que 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;

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

Está correto APENAS o que consta em:

a) I.

b) I e II.

c) I e III.

d) II e III.

e) I, II e III.

Comentários:

Questão de revisão. Todos estão corretos.

Gabarito: "e"

7. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

As instituições devem elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes. O plano deve abordar, entre outras coisas, EXCETO

a) a efetividade da implementação das ações.

b) o resumo dos resultados obtidos na implementação.

c) as diretrizes da política de segurança cibernética.

d) os incidentes relevantes ocorridos.

e) os resultados dos testes de continuidade de negócios

Comentários:

As diretrizes (letra "c") devem constar no próprio plano, e não estão entre os itens que devem constar no relatório anual.

As instituições devem elaborar **relatório anual** sobre a implementação do plano de ação e de resposta a incidentes, abordando, entre outras coisas:

- a efetividade da implementação das ações;
- o resumo dos resultados obtidos na implementação;
- os incidentes relevantes ocorridos
- os resultados dos testes de continuidade de negócios.

Gabarito: "a"

8. (2021/CESGRANRIO/CAIXA ECONÔMICA FEDERAL/Técnico Bancário - TI)

A 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.

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:

Questão bem objetiva, sem muito mais a comentar, além de trazer o prazo correto de revisão:

> *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: "c"

9. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A política de segurança cibernética e o plano de ação, previstos na norma, devem
a) ser aprovados pela diretoria ou, em caso de inexistência, pelo conselho de administração.
b) ser documentados e revisados, no mínimo, anualmente.
c) ficar à disposição do Banco Central pelo prazo de dez anos.
d) ser implementados apenas por instituições financeiras.
e) ser assinados pelos clientes no momento da abertura da conta.

Comentários:

Vejamos essas alternativas.

a) ser aprovados pela diretoria ou, em caso de inexistência, pelo conselho de administração.

Errado. É o contrário: quem aprova é o conselho e, se não existir conselho, fica a cargo da diretoria.

b) ser documentados e revisados, no mínimo, anualmente.

Certo. Aqui está nosso gabarito.

c) ficar à disposição do Banco Central pelo prazo de dez anos.

Errado. O prazo é de cinco anos.

d) ser implementados apenas por instituições financeiras.

Errado. Vale também para outras instituições autorizadas a funcionar pelo Banco Central.

e) ser assinados pelos clientes no momento da abertura da conta.

Errado. Inventei isso. Os clientes não precisam assinar esses documentos.

Gabarito: "b"

10. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A respeito da norma, assinale a opção CORRETA.

a) Os serviços de computação em nuvem abrangem, apenas, o processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais.

b) A implantação ou execução de aplicativos desenvolvidos pela instituição contratante, utilizando recursos computacionais do prestador de serviços, não está incluída no conceito de computação em nuvem.

c) A instituição contratante é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços.

d) As instituições devem assegurar que suas políticas contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, apenas no País.

e) A contratação dos serviços de computação em nuvem deve ser comunicada previamente pelas instituições ao Banco Central do Brasil.

Comentários:

Vamos analisar essas alternativas.

a) Os serviços de computação em nuvem abrangem, apenas, o processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais.

Errado, por causa do "apenas". Abrange também:

> *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, dos aplicativos** implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.*

b) A implantação ou execução de aplicativos desenvolvidos pela instituição contratante, utilizando recursos computacionais do prestador de serviços, não está incluída no conceito de computação em nuvem.

Errado. É o item II da transcrição acima e, portanto, foi incluída no conceito da Resolução.

c) A instituição contratante é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços.

Certo!

d) As instituições devem assegurar que suas políticas contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, apenas no País.

Errado. Vale para contratação no exterior também.

e) A contratação dos serviços de computação em nuvem deve ser comunicada previamente pelas instituições ao Banco Central do Brasil.

Errado. A comunicação deve ocorrer em até 10 dias após a contratação.

Gabarito: "c"

11. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A respeito das competências do Banco Central, é correto afirmar que a autarquia pode

a) estabelecer o os requisitos e os procedimentos para o compartilhamento de informações.

b) determinar prazos mínimos para reinício ou normalização das atividades ou dos serviços relevantes interrompidos.

c) ter sua atuação de fiscalização limitada por cláusula de sigilo entre as instituições e a empresa contratada.

d) impor, para qualquer empresa, restrições para contratação de serviços na nuvem caso detecte irregularidades.

e) exigir, apenas da instituição contratante, certificações e outros requisitos técnicos na prestação dos serviços na nuvem.

Comentários:

A letra "a" está correta. O BCB pode:

- **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;
  - 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 desta Resolução.
- 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 das normas, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação dos referidos serviços.

Então vamos deixar bem claros os erros nas demais alternativas.

b) determinar prazos mínimos para reinício ou normalização das atividades ou dos serviços relevantes interrompidos.

Errado. É o prazo máximo que pode ser determinado. Não faria sentido falar em prazo mínimo.

c) ter sua atuação de fiscalização limitada por cláusula de sigilo entre as instituições e a empresa contratada.

Errado! Inclusive, isso é motivo para imposição de restrição à contratação.

d) impor, para qualquer empresa, restrições para contratação de serviços na nuvem caso detecte irregularidades.

Errado. O BC só pode impor essas restrições para instituições financeiras ou outras instituições cuja autorização para funcionamento esteja sob sua responsabilidade. Não é "qualquer empresa", portanto.

e) exigir, apenas da instituição contratante, certificações e outros requisitos técnicos na prestação dos serviços na nuvem.

Errado. Pode exigir da contratada também.

Gabarito: "a"

LISTA DE QUESTÕES

1. (2019/CAE-CFC/Cadastro Nacional de Auditores Independentes BCB)

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.

2. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A política de segurança cibernética deve assegurar, em relação aos dados, EXCETO

a) disponibilidade.

b) integridade.

c) portabilidade.

d) segurança.

e) confidencialidade

3. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

Sobre esse assunto, de acordo Resolução, a política de segurança 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. as políticas de segurança pública do município em que está localiza a agência ou filial

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

Estão CERTOS apenas 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.

e) I, II e IV, apenas

4. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A Resolução determina que a política de segurança cibernética deve contemplar os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética, abrangendo

a) a prevenção de compartilhamento de informações

b) a vedação à criptografia

c) a realização de varreduras posteriores à detecção de vulnerabilidades

d) a proteção contra cópias de segurança dos dados e das informações

e) o estabelecimento de mecanismos de rastreabilidade

5. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A divulgação da política de segurança deve

a) ser realizada sempre em linguagem técnica, adequada ao público especializado.

b) ter nível de detalhamento máximo, a todos os públicos.

c) ser vedada, por tratar de temas sensíveis.

d) ser realizada, de forma resumida, ao público.

e) ser restrita aos funcionários e contratados.

6. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A respeito do plano de ação e de resposta a incidentes, a norma determina que 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;

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

Está correto APENAS o que consta em:

a) I.

b) I e II.

c) I e III.

d) II e III.

e) I, II e III.

7. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

As instituições devem elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes. O plano deve abordar, entre outras coisas, EXCETO

a) a efetividade da implementação das ações.

b) o resumo dos resultados obtidos na implementação.

c) as diretrizes da política de segurança cibernética.

d) os incidentes relevantes ocorridos.

e) os resultados dos testes de continuidade de negócios

8. (2021/CESGRANRIO/CAIXA ECONÔMICA FEDERAL/Técnico Bancário - TI)

A 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.

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

9. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A política de segurança cibernética e o plano de ação, previstos na norma, devem

a) ser aprovados pela diretoria ou, em caso de inexistência, pelo conselho de administração.

b) ser documentados e revisados, no mínimo, anualmente.

c) ficar à disposição do Banco Central pelo prazo de dez anos.

d) ser implementados apenas por instituições financeiras.

e) ser assinados pelos clientes no momento da abertura da conta.

10. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A respeito da norma, assinale a opção CORRETA.

a) Os serviços de computação em nuvem abrangem, apenas, o processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais.

b) A implantação ou execução de aplicativos desenvolvidos pela instituição contratante, utilizando recursos computacionais do prestador de serviços, não está incluída no conceito de computação em nuvem.

c) A instituição contratante é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços.

d) As instituições devem assegurar que suas políticas contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, apenas no País.

e) A contratação dos serviços de computação em nuvem deve ser comunicada previamente pelas instituições ao Banco Central do Brasil.

11. (2021/PROF. CELSO NATALE)

A Resolução CMN nº 4.893, de 26/2/2021, 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.

A respeito das competências do Banco Central, é correto afirmar que a autarquia pode

a) estabelecer o os requisitos e os procedimentos para o compartilhamento de informações.

b) determinar prazos mínimos para reinício ou normalização das atividades ou dos serviços relevantes interrompidos.

c) ter sua atuação de fiscalização limitada por cláusula de sigilo entre as instituições e a empresa contratada.

d) impor, para qualquer empresa, restrições para contratação de serviços na nuvem caso detecte irregularidades.

e) exigir, apenas da instituição contratante, certificações e outros requisitos técnicos na prestação dos serviços na nuvem.

GABARITO

1. A
2. C
3. E
4. E
5. D
6. E
7. A
8. C
9. B
10. C
11. A

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.