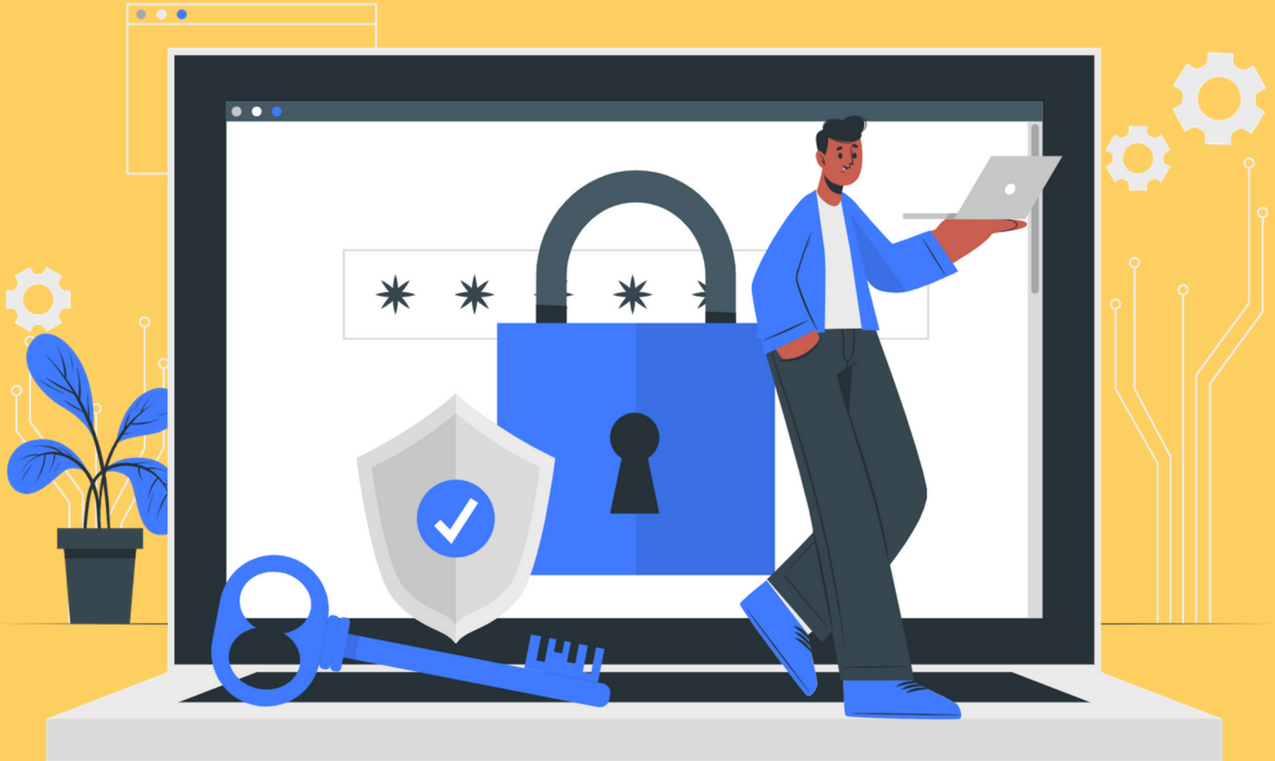
CARTILHA

Entenda os principais pontos da Resolução CMN 4.893/2021 do Banco Central do Brasil

Atualizações trazidas pela Resolução CMN 4.893/2021 que dispõe sobre a política de segurança cibernética e os requisitos para a contratação de serviços de processamento e de armazenamento de dados e de computação em nuvem



OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

SUMÁRIO

Introdução 3

Principais pontos atualizados pela Resolução CMN nº 4.893/2021 4

Conceitos básicos 6

- Política de Segurança Cibernética 6
- Plano de Ação e de Resposta a Incidentes 10
- Incidentes relevantes 10
- Gerenciamento de crise e Plano de Continuidade de Negócios 11

Requisitos obrigatórios na contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem 12

Requisitos adicionais para contratação de processamento e armazenamento de dados e de computação em nuvem prestados no exterior 14

Mecanismos para implementação e efetividade da Resolução 15

Observações importantes 16

Créditos 17

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Introdução

O Banco Central do Brasil (BACEN), alinhado à constante evolução tecnológica e objetivando assegurar um ambiente aderente às normas de segurança cibernética e de proteção de dados pessoais, editou a Resolução CMN nº 4.893, de 26 de fevereiro de 2021, que dispõe sobre a estruturação da 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 por ele autorizadas a funcionar (Resolução CMN nº 4.893/2021).

A Resolução entra em vigor no dia 1º de julho de 2021 e traz atualizações nos normativos sobre a política já existente, revogando as Resoluções nº 4.658/2018 e 4.752/2019. Nesta cartilha, abordamos, por meio de uma linguagem prática e visual, alguns conceitos básicos relacionados à segurança cibernética no âmbito do BACEN e os principais pontos de alteração trazidos pela nova Resolução.

Principais pontos atualizados pela Resolução CMN nº 4.893/2021

OPICE BLUM

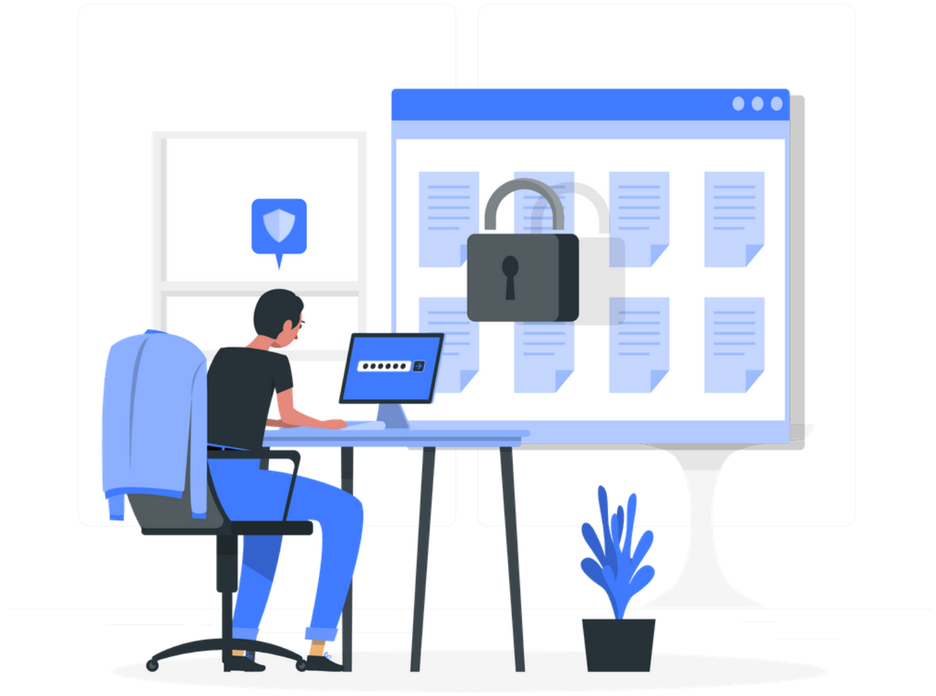
OPICE BLUM | BRUNO | VAINZOF

A Resolução CMN nº 4.893/2021 não altera a essência da Resolução 4.658/2018. Os principais pontos de alteração da nova Resolução estão relacionados ao gerenciamento de crise.

Gerenciamento de crise: as instituições financeiras e demais instituições autorizadas pelo BACEN (aqui chamadas de "IFs ou instituições autorizadas") devem estabelecer e documentar os critérios que configurem uma situação de crise.

1. Em caso de uma situação de crise que implique em incidentes ou interrupções, o BACEN deverá ser comunicado tempestivamente pela instituição e informado sobre as providências para a retomada das atividades

2. A documentação do gerenciamento de crise deverá ficar à disposição do BACEN pelo prazo de 5 anos, conforme artigos 20, parágrafo único, e 23, inciso IX

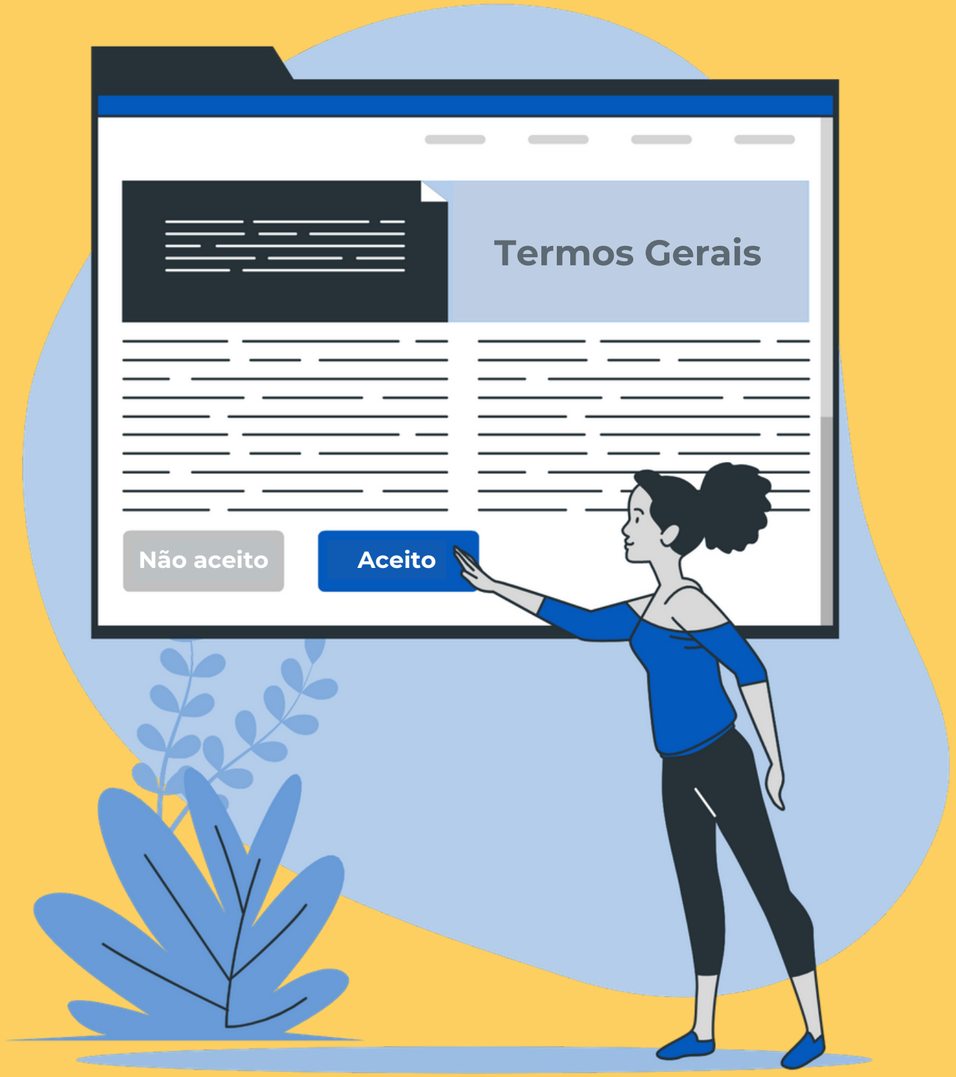


Conceitos básicos

É importante recapitular alguns conceitos disciplinados pelo BACEN, por meio da Resolução 4.658/2018, e que foram mantidos na Resolução CMN 4.893/2021.

A seguir, trazemos alguns dos principais conceitos envolvendo segurança cibernética e a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Política de Segurança Cibernética é o documento que todas as instituições financeiras e demais instituições autorizadas a funcionar pelo BACEN devem elaborar para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.



Os requisitos mínimos que a Política deve apresentar são:

1. Os objetivos da IF ou instituição autorizada na contratação dos serviços de processamento e armazenamento de dados e de computação em nuvem

2. Os procedimentos e controles para reduzir a vulnerabilidade a incidentes, inclusive no desenvolvimento de sistemas de informação e na adoção de novas tecnologias pela IF ou instituição autorizada, que devem abranger:

- Autenticação, criptografia, prevenção e a detecção de intrusão
- Prevenção de vazamento de informações
- Realização periódica de testes e varreduras para detecção de vulnerabilidades
- Proteção contra softwares maliciosos
- Mecanismos de rastreabilidade
- Controles de acesso e de segmentação da rede de computadores
- Manutenção de cópias de segurança (backup) dos dados e das informações

3. Os controles específicos para garantir a **segurança das informações sensíveis**

4. Orientações para o correto registro, análise de causa e do impacto, tratamento adequado de incidentes relevantes para as atividades da IF ou instituição autorizada, **inclusive informações recebidas de empresas prestadoras de serviços a terceiros**

5. Diretrizes para:

- Elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;
- Procedimentos e controles voltados à prevenção e tratamento dos incidentes, a serem adotados por **empresas prestadoras de serviços a terceiros que realizem o tratamento de dados ou informações sensíveis ou que sejam relevantes** para a condução das atividades operacionais da IF ou instituição autorizada;
- Classificação dos dados e das informações quanto à relevância; e
- Parâmetros utilizados na definição da relevância dos incidentes.

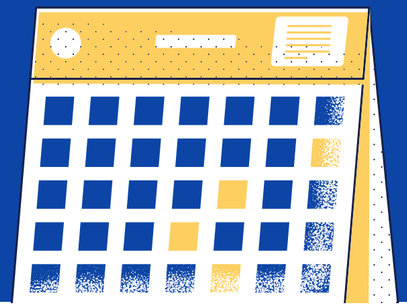
6. Mecanismos para disseminação da cultura de segurança cibernética na IF ou instituição autorizada, incluindo:

- Programas de capacitação e avaliação periódica de pessoal; e
- Prestação de informações a clientes e usuários sobre os cuidados na utilização de produtos e serviços financeiros.

7. Iniciativas para compartilhamento de informações sobre os incidentes relevantes com as demais IFs ou instituições autorizadas e o BACEN

Plano de Ação e de Resposta a Incidentes

É o documento que descreve os métodos para reduzir o nível de exposição a incidentes da IF ou instituição autorizada



Os requisitos mínimos do Plano são:

1. As ações da IF ou instituição autorizada para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética

2. 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

3. Área responsável pelo registro e controle dos efeitos de incidentes relevantes

Incidentes relevantes

São situações de crise enfrentadas pela IF ou instituição autorizada, decorrentes da violação em seus protocolos de segurança, como acesso não autorizado, acidental ou ilícito que possa ocasionar destruição, perda, alteração, vazamento, fraudes ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, expondo a riscos os direitos e as liberdades dos titulares de dados pessoais afetados, além da própria IF ou instituição autorizada, que também fica exposta a riscos financeiros (multas, ações judiciais) e de imagem.

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Gerenciamento de crise

É um conjunto de práticas com objetivo de lidar **com cenários de anormalidade**, internos ou externos à IF ou instituição autorizada, que possam causar **prejuízos financeiros, de imagem e/ou de reputação**, a fim de minimizar os impactos negativos e identificar oportunidades de melhoria.

Alguns exemplos de situação de crise: **acidentes graves** envolvendo colaboradores, **ataques de cibercriminosos** que possam alterar ou interromper processos internos causando incidentes relevantes, **vazamento de dados**, desastres naturais e falhas consideráveis da estrutura interna.

Ter uma política de gerenciamento de crise é fundamental para a manutenção do sucesso dos negócios das IFs ou instituições autorizadas.

A Resolução CMN nº 4.893/2021 dedicou o artigo 20 especificamente a esse assunto, destacando a necessidade de as IFs ou instituições autorizadas estabelecerem e documentarem os critérios que configurem situação de crise, assim como aqueles necessários para o desenvolvimento do Plano de Continuidade de Negócios.

Plano de Continuidade de Negócios

Reúne os procedimentos que as IFs ou instituições autorizadas devem documentar e adotar como um guia para enfrentar a situação de crise. A Resolução CMN nº 4.893/2021 prevê como **requisitos** do Plano de Continuidade de Negócios das IFs ou instituições autorizadas (art. 20):

1

O **tratamento para mitigar os efeitos** dos incidentes relevantes e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados;

2

O **prazo para reinício ou normalização** das atividades ou dos serviços relevantes interrompidos;

3

A **comunicação tempestiva ao BC** das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configurem situação de crise e as providências para o reinício das suas atividades.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

Requisitos obrigatórios na contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem

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

B Políticas, estratégias e estruturas para gerenciamento de riscos que contemplem a contratação no País ou no exterior

C Práticas de governança e procedimentos que assegurem a verificação de capacidade da empresa e aderência às exigências da IF ou instituição autorizada e da regulamentação em vigor antes da contratação, considerando:

I **Criticidade de serviço; e**

II **Sensibilidade dos dados.**

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

D A IF ou instituição autorizada como responsável pela confiabilidade, integridade, disponibilidade dos serviços contratados

E Obrigação de notificar a subcontratação de serviços relevantes para a IF ou instituição autorizada

F **Comunicação ao BACEN da contratação ou atualização contratual de serviços relevantes.** Essa comunicação deve ser realizada em **até 10 dias após a contratação dos serviços ou atualização contratual**, contendo:

i. Denominação da empresa contratada;

ii. Detalhamento dos serviços contratados;

iii. Indicação dos países e das regiões em cada país onde os serviços poderão ser prestados;

iv. Dados que serão armazenados, processados e gerenciados.

Obs.: os requisitos citados não se aplicam à contratação de sistemas operados por câmaras, por prestadores de serviços de compensação e de liquidação ou por entidades que exerçam atividades de registro ou de depósito centralizado.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

Requisitos adicionais para contratação dos serviços de processamento e armazenamento de dados e de computação em nuvem prestados no exterior

Existência de convênio entre o BACEN com autoridades dos países e regiões onde os dados serão armazenados, gerenciados e processados

Obs.: caso não exista convênio, é necessário solicitar uma autorização do BACEN no mínimo 60 dias antes da contratação ou atualização de contrato já existente, assegurando e evidenciando documentalmente 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 da IF ou instituição autorizada e do BACEN aos dados e informações.

Não causar prejuízos ao funcionamento regular da IF ou instituição autorizada nem dificultar a atuação do BACEN

Prever plano de continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Mecanismos para implementação e efetividade da Resolução

- Definição de processos, testes e trilhas de auditoria;
- Definição de métricas e indicadores adequados; e
- Identificação e correção de eventuais deficiências.

Esses mecanismos devem ser submetidos a testes periódicos pela auditoria interna, quando isso for aplicável, e compatíveis com os controles internos da IF ou instituição autorizada.

Observações Importantes

Devem ficar à disposição do BACEN pelo prazo de 5 anos:

IMPORTANTE!

A IF ou instituição autorizada que já tenha contratado serviços de processamento e armazenamento de dados e de computação em nuvem na vigência da Resolução nº 4.658/2018 deve adequar os contratos firmados com seus prestadores de serviços até 31 de dezembro de 2021

1. A Política de Segurança Cibernética;
2. A ata de reunião do conselho de administração ou diretoria (no caso de adoção de política única por conglomerado/sistema cooperativo de crédito);
3. Plano de Ação e de Resposta a Incidentes;
4. O relatório anual;
5. A documentação sobre os procedimentos de contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
6. A documentação relativa à aprovação do convênio entre o BACEN, no caso de serviços prestados no exterior;
7. Contratos de prestação de serviços relevantes, sendo o prazo contado a partir do encerramento dos respectivos contratos;
8. Os dados, registros e informações sobre os mecanismos de acompanhamento e controle, sendo o prazo contado a partir da implementação;
9. A documentação relativa ao gerenciamento de riscos.

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

CRÉDITOS

Sócios

José Roberto Opice Blum, Renato Opice Blum, Marcos Gomes da Silva Bruno, Rony Vainzof, Camilla Jimene, Caio César Carvalho Lima e Danielle Serafino

Autoria

Florence Terada e Camila do Amaral Cerqueira

Revisão

Rony Vainzof, Caio César Carvalho Lima, Bruno Toranzo e Yasmin Brandão

Coordenação editorial

Bruno Toranzo

Arte e design

Paola Melhem Cosentino

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF