

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Versão 3.0 – 01/2023



## 1. OBJETIVO

Esta Política de Segurança da Informação e Segurança Cibernética (“Política”) tem o objetivo de estabelecer diretrizes que permitem à CELCOIN INSTITUIÇÃO DE PAGAMENTO S.A. “CELCOIN” preservar e proteger as informações de seus clientes, funcionários, prestadores de serviços, partes interessadas e da própria CELCOIN contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade da CELCOIN a incidentes, e também dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

A CELCOIN deve implementar e manter esta Política 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.

Esta Política será compatível com:

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

A CELCOIN designará diretor responsável por esta Política e pela execução do plano de ação e de resposta a incidentes.

## 2. ABRANGÊNCIA

A Política se aplica a todos os administradores, diretores e conselheiros (coletivamente “Alta Administração”), funcionários e prestadores de serviço da CELCOIN (coletivamente, inclusive a Alta Administração, denominados simplesmente por “Colaboradores”).

## 3. NORMAS APLICÁVEIS

Circular nº 3.909, de 16 de agosto de 2018, do Banco Central do Brasil.

## 4. APROVAÇÃO E REVISÃO

Esta Política foi aprovada e revisada pela Alta Administração e será revisada periodicamente. A Política também será alterada para contemplar quaisquer alterações regulatórias e outras obrigações legais.

## 5. TERMOS E DEFINIÇÕES

**Ativos:** todas as formas de criação, processamento, armazenamento, transmissão e exclusão de informações. Os Ativos podem ser documentos impressos, sistemas, softwares, banco de dados, arquivos digitais, dispositivos móveis etc.

**Bacen:** Banco Central do Brasil.

**Instituição de Pagamento:** para fins desta Política, é o emissor de moeda eletrônica, cuja atividade consiste em gerenciar a conta de pagamento de usuários, utilizada para o pagamento de transações pré-pagas e pós-paga.

**Log:** registro de eventos de um sistema.

**Segurança da Informação:** conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos da CELCOIN.

**Segurança Cibernética:** conjunto de tecnologias e processos desenvolvidos para proteger os sistemas internos, computadores, redes e dados da CELCOIN contra ataques, danos, ameaças ou acesso não autorizado.

**LGPD:** Lei Geral de Proteção de Dados, lei 13.709/18;

**Dado Pessoal:** Esta política considera dado pessoal exatamente como à LGPD- art. 5º, inciso I;

**Dado Pessoal Sensível:** Esta política considera dado pessoal exatamente como à LGPD- art. 5º, inciso II;

**Operador:** Esta política considera dado pessoal exatamente como à LGPD- art. 5º, inciso VII;

**Colaborador:** Funcionário, estagiário, terceiro contratado para prestar serviço à CELCOIN;

## 6. PRINCÍPIOS

A CELCOIN tem o compromisso garantir a segurança e tratamento adequado das informações. Para tanto, nossas atividades se baseiam nos seguintes princípios:

**Confidencialidade:** garantia de que somente pessoas autorizadas terão acessos às informações e apenas quando houver necessidade;

**Integridade:** garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente;

**Disponibilidade:** garantia de que a informação estará disponível às pessoas autorizadas sempre que for necessário.

## 7. DIRETRIZES GERAIS

São diretrizes desta Política:

- Com o objetivo de garantir os objetivos desta Política, os procedimentos de Segurança da Informação e Segurança Cibernética seguirão as seguintes diretrizes:
- Assegurar que não haja acessos indevidos, modificações, destruições ou divulgações não autorizadas das informações. Para tanto, o acesso do Colaborador deve ser pessoal, intransferível e restrito aos recursos necessários para realizar suas atribuições na CELCOIN.
- Cada Colaborador, quando aplicável, receberá uma senha pessoal de acesso e ficará responsável por manter sua senha em sigilo para evitar acesso indevido às informações que estão sob sua responsabilidade. A CELCOIN adotará mecanismos que assegurem a resiliência, troca periódica e guarda de histórico de senhas.
- Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador por meio do canal oficial de contato com a área de Segurança da Informação da CELCOIN [security@celcoin.com.br](mailto:security@celcoin.com.br)

- Assegurar que todas as informações e dados pessoais sejam tratadas de maneira ética e sigilosa e que sejam adotadas medidas capazes de evitar acessos indevidos, modificações, destruições ou divulgações não autorizadas.
- Assegurar que as informações e dados pessoais sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização.
- Neste contexto, assegurar que as informações e dados pessoais estejam protegidas de maneira a garantir que a CELCOIN atenda todos os requisitos da LGPD – Lei Geral de Proteção de Dados.
- Assegurar os procedimentos e controles adotados para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de Segurança Cibernética, tais como, 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.
- Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam a segurança das informações sensíveis.
- Assegurar o registro, análise da causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades de uma Instituição de Pagamento.
- Assegurar a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;
- Definir os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes que devem ser adotados pelos prestadores de serviços e terceiros que manuseiem dados e/ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da CELCOIN;
- Classificação periódica dos dados e das informações quanto à sua relevância e sensibilidade;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;

- Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo:
  - A implementação de programas de capacitação e de avaliação periódica de pessoal;
- A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos.
- Assegurar as iniciativas para compartilhamento de informações sobre os incidentes relevantes, com Instituições de Pagamento, instituições financeiras e demais instituições autorizadas a funcionar pelo Bacen.
- Assegurar o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes de informações recebidas de empresas prestadoras de serviços a terceiros.
- Contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela CELCOIN e por esta Política.

## 8. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A fim de assegurar que todas as diretrizes acima sejam cumpridas e que os princípios de Segurança da Informação, privacidade de dados e de Segurança Cibernética sejam devidamente seguidos, a CELCOIN adotará políticas e procedimentos para os processos elencados a seguir.

### 8.1. Política de Senhas

A fim de garantir maior segurança no processo de geração e gestão de senhas. A CELCOIN estabelece que as senhas geradas devem obedecer aos critérios abaixo:

As senhas geradas devem obrigatoriamente conter no mínimo:

- 8 dígitos;
- Combinação de letra MAIÚSCULAS, minúsculas, números e caracteres especiais;
- Deverá ser alterada a senha padrão no primeiro login;
- Deverá expirar a cada 60 dias;

- Na troca da senha, não poderá repetir as últimas duas senhas utilizadas.

## 8.2. Gestão de ativos

Os Ativos devem ser inventariados e protegidos de acessos indevidos ou ameaças que possam comprometer o negócio. Para tanto, o acesso às salas com documentos físicos deve ser limitado, por meio de mecanismos de autenticação e autorização de acesso, destinados a impedir o acesso de indivíduos não autorizados.

Os Ativos devem ser utilizados tão somente para a finalidade devidamente autorizada. A CELCOIN deve assegurar proteção aos Ativos durante todo o seu ciclo de vida, a fim de garantir que os princípios da confidencialidade, integridade e disponibilidade sejam cumpridos integralmente.

## 8.3. Autenticação

A CELCOIN adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

## 8.4. Segmentação de rede

A CELCOIN deve adotar mecanismos internos para a segmentação de rede para proteger seus dados de ataques cibernéticos e determinar que todos os computadores conectados à rede corporativa não estejam acessíveis diretamente pela Internet.

## 8.5. Classificação da informação

As informações devem ser classificadas segundo sua criticidade e sensibilidade para o negócio, titulares de dados pessoais e seus clientes. Portanto, a CELCOIN deve adotar a seguinte classificação:

- **Informação Pública:** aquela que pode ser acessada por todos, sem restrição. São exemplos de Informação Pública: dados divulgados ao mercado e promocionais;

- **Informação Interna:** aquela que pode ser acessada somente por Colaboradores da CELCOIN. São exemplos de Informação Interna: normas, procedimentos e formulários da CELCOIN;
- **Informação Restrita:** aquela que pode ser acessada somente por Colaboradores que precisam dela para desempenhar suas atribuições. São exemplos de Informação Restrita: contratos e documentos estratégicos da CELCOIN.
- Toda informação contendo dado pessoal simples deverá ser classificada como Informação Restrita.
- **Informação Confidencial:** aquela que pode ser acessada somente por Colaboradores que tenham permissão de acesso ou que necessitem dela para um propósito específico. São exemplos de Informação Confidencial: plano estratégico e informações de clientes.
- Toda informação que contenha dado pessoal sensível deverá ser classificada como informação confidencial.

## 8.6. Controles de Acessos

A CELCOIN adotará controles de acesso em toda infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados e aos sistemas internos. Desta forma, a CELCOIN deve implementar mecanismos para a autenticação de usuários, manutenção de segregação de funções e rastreabilidade de acesso, de forma a garantir procedimentos internos adequados e consistentes.

## 9. GESTÃO DE RISCOS

A CELCOIN possui processo para análise de vulnerabilidades, ameaças e impactos sobre os Ativos de informação para, diante de um incidente, adotar as medidas adequadas para minimizar os danos causados.

## 10. GESTÃO DE FORNECEDORES

A CELCOIN realizará a devida diligência de verificação de todos os seus prestadores de serviços, fornecedores, provedores e parceiros com relação a controles de Segurança da Informação, privacidade de dados e Segurança Cibernética, em especial aqueles que processam e armazenam dados da CELCOIN, com a finalidade de verificar



o nível de maturidade dos padrões de segurança e o plano de tratamento de incidentes adotados.

A CELCOIN disponibiliza o canal oficial [security@celcoin.com.br](mailto:security@celcoin.com.br) para que seus prestadores de serviços, fornecedores, provedores, operadores e parceiros comuniquem incidentes de Segurança da Informação, privacidade de dados e Segurança Cibernética que estejam relacionados às informações da CELCOIN.

## 11. SEGURANÇA FÍSICA DO AMBIENTE

A CELCOIN implementará sistema para controle de acesso dos Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros aos locais restritos. Os equipamentos e instalações de processamento de informação crítica ou sensível deverão ser mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

## 12. BACKUP E GRAVAÇÃO DE LOG

A CELCOIN adotará uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades.

A CELCOIN também realizará gravação de logs de dados que permitam a rastreabilidade do acesso e a identificação do criador, data, meios de acessos e informações acessadas. As informações dos logs devem ser protegidas contra alterações e acessos não autorizados.

## 13. PROTEÇÃO CONTRA VÍRUS, ARQUIVOS E SOFTWARES MALICIOSOS

A CELCOIN adotará mecanismos para prevenir que vírus e outros tipos de *software* e condutas maliciosas (e.g., *phishing*, *spam*, etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham a CELCOIN a vulnerabilidades.

## 14. TESTES DE VARREDURA PARA DETECÇÃO DE VULNERABILIDADE

A CELCOIN se preocupa em identificar e eliminar as vulnerabilidades de seus sistemas e servidores para assegurar a integridade do ambiente dos processos de negócio. Para tanto, promoverá monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas

## **15. CRIPTOGRAFIA**

Os Ativos de informação da CELCOIN serão protegidos com criptografia adequada, a fim de se garantir confidencialidade e integridade em todo o ciclo de vida da informação, em conformidade com os padrões de segurança dos órgãos reguladores.

## **16. PLANO DE CONTINUIDADE**

A CELCOIN realiza plano de continuidade dos serviços prestados a partir da adoção de um conjunto preventivo de estratégias e planos de ação para garantir que os serviços essenciais da CELCOIN sejam devidamente identificados e preservados após a ocorrência de uma contingência. Adicionalmente, assegurando que o plano seja testado a intervalos planejados, não superior a um ano.

## **17. INCIDENTES DE SEGURANÇA**

### **17.1. Classificação de relevância dos incidentes**

A CELCOIN classificará os incidentes de segurança da informação, e incidentes de segurança envolvendo dados pessoais segundo sua relevância e conforme a classificação das informações, dados pessoais e titulares envolvidos, e o impacto na continuidade dos negócios da CELCOIN.

### **17.2. Gestão de incidentes**

Convém que a organização tenha procedimentos implementados para garantir uma reação ordenada e eficaz aos eventos e pontos fracos de segurança da informação relatados. Os procedimentos devem garantir que todos os eventos relatados sejam revisados e investigados quando apropriado, que os procedimentos de recuperação sejam acionados e que as funções de senioridade adequada estejam envolvidas nas revisões.

Todos os incidentes ou suspeita de incidentes identificados por um colaborador, cliente, prestador de serviços, fornecedor, provedor ou parceiro serão imediatamente comunicados à área responsável. A comunicação deverá ser feita por meio do canal oficial de Segurança da Informação na CELCOIN, através do e-mail [security@celcoin.com.br](mailto:security@celcoin.com.br).

Os incidentes reportados serão classificados segundo o risco que representam para a CELCOIN e o impacto na continuidade dos negócios da CELCOIN. Além disso, serão devidamente registrados, tratados e comunicados, de acordo com os procedimentos da área de Segurança da Informação e a legislação vigente.

A CELCOIN adotará procedimentos para mitigar os efeitos dos incidentes relevantes e minimizar a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

Caso haja incidentes relevantes ou interrupção dos serviços relevantes, a CELCOIN comunicará o Bacen e adotará medidas necessárias para que as suas atividades sejam reiniciadas.

### **17.3. Plano de compartilhamento de incidentes**

Sem prejuízo do dever de sigilo, da livre concorrência e preservando segredos comerciais, a CELCOIN adotará iniciativas para o compartilhamento de informações sobre incidentes relevantes com outras Instituições de Pagamento por meio dos canais adotados pelas instituições.

As informações compartilhadas também estarão disponíveis ao Bacen.

### **17.4. Plano de ação e resposta a incidentes**

A CELCOIN estabelecerá plano de ação e de resposta a incidentes visando à implementação desta Política, que abrange, minimamente:

- As ações a serem desenvolvidas para adequar as estruturas organizacional e operacional às diretrizes desta Política;
- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

## 17.5. Relatório anual de incidentes

A CELCOIN elaborará relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro. O relatório abordará:

- A efetividade da implementação das ações de adequação suas estruturas organizacional e operacional;
- 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, em conformidade com as diretrizes desta Política;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- Os resultados dos testes de continuidade dos serviços de pagamento prestados, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório anual de incidentes será apresentado ao Conselho de Administração ou, na sua inexistência, à Diretoria da CELCOIN até 31 de março do ano seguinte ao da data-base.

## 18. MECANISMOS DE RASTREABILIDADE

A CELCOIN adotará controles específicos para promover a rastreabilidade da informação, principalmente que busquem garantir a segurança das informações sensíveis.

## 19. REGISTRO DE IMPACTO

A CELCOIN realizará registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da CELCOIN, que devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

## 20. TREINAMENTOS E CONSCIENTIZAÇÃO

A CELCOIN preza por uma cultura de Segurança da Informação, privacidade de dados e Segurança Cibernética. Dessa forma, serão adotados políticas e procedimentos para

a difusão dos princípios e diretrizes integrantes desta Política, garantindo-se a capacitação e conscientização para todos os seus Colaboradores.

A CELCOIN promoverá a ampla divulgação desta Política a todos os seus Colaboradores e o público em geral, bem como 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, incluindo a prestação de informações aos usuários finais sobre medidas de precaução para a utilização dos produtos e serviços oferecidos.

Além disto, a Alta Administração da CELCOIN deverá difundir a cultura de Segurança da Informação e Segurança Cibernética para promover melhorias contínuas em seus processos internos, a fim de evitar quaisquer incidentes relacionado à Segurança da Informação e Segurança Cibernética.

## **21. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM**

### **21.1. Seleção de terceiros**

O processamento e armazenamento de dados e computação em nuvem será realizado por meio de terceiros localizados no Brasil ou no exterior. A contratação de terceiros deve ser realizada por meio da aferição da capacidade do prestador de serviço para realizar as atividades em cumprimento com a legislação e regulamentação aplicável. Desta forma, a CELCOIN adotará procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar:

- O cumprimento da legislação e da regulamentação em vigor, incluindo a Lei Geral de Proteção de Dados, no que tange a proteção dos dados pessoais utilizados para o processamento de transações;
- Garantia que, mesmo que os dados e informações sejam hospedados no exterior, que cumpram todos os requisitos da legislação brasileira;
- O acesso da CELCOIN aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

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

Na avaliação da relevância do serviço a ser contratado, a CELCOIN também deverá considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado. Todos os procedimentos deverão ser documentados.

Ademais, a CELCOIN adotará recursos e medidas necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso dos recursos providos pelo potencial prestador de serviços.

## **21.2. Execução de aplicativos pela internet**

No caso da execução de aplicativos por meio da internet, a CELCOIN deverá assegurar que o potencial prestador dos serviços adote controles para a proteção contra os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

## **21.3. Serviço de computação em nuvem**

Os serviços de computação em nuvem disponibilizados à CELCOIN, sob demanda e de maneira virtual, deverão incluir um ou mais serviços conforme descritos abaixo:

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

A CELCOIN é responsável, em conjunto com o prestador de serviços, pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem será comunicada pela CELCOIN ao Bacen, nos termos da legislação em vigor.

#### **21.4. Contratação de serviços de computação em nuvem do exterior**

Em caso de contratação de serviços de processamento, armazenamento de dados e de computação em nuvem no exterior, a CELCOIN observará os seguintes requisitos:

- Existência de convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países onde os serviços serão prestados;
- Verificação de que a prestação dos serviços não causará prejuízos ao seu regular funcionamento nem embaraço à atuação do Bacen;
- Definição dos países e regiões em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados. Essa definição deverá ocorrer antes da contratação dos serviços; e
- Previsão de alternativas para a continuidade dos serviços de pagamento prestados, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

Caso não haja convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países em que os serviços serão prestados, a CELCOIN solicitará autorização do Bacen para a contratação do serviço. O prazo para solicitar autorização é de 60 dias anteriores à contratação. Caso haja alterações contratuais que impliquem em modificação das informações, a CELCOIN solicitará autorização 60 dias antes da alteração contratual.

A CELCOIN tem a responsabilidade de assegurar que a legislação e a regulamentação nos países em que os serviços serão prestados não restrinjam ou impeçam o acesso da CELCOIN e do Bacen aos dados e às informações. A comprovação do atendimento aos requisitos e o cumprimento desta exigência deverão ser documentados.

## 21.5. Contrato de prestação de serviços

A CELCOIN deverá assegurar que os contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem prevejam:

- A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados;
- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;
- Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou à CELCOIN, bem como a exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos;
- O acesso da CELCOIN às informações fornecidas pela empresa contratada; bem como as informações relativas às certificações e aos relatórios de auditoria especializada e informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A obrigação da empresa contratada notificar a CELCOIN sobre a subcontratação de serviços relevantes para a CELCOIN;



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

Em caso de decretação de regime de resolução da CELCOIN pelo Bacen, o contrato de prestação de serviços deve prever:

- A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, acordos, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso, que estejam em poder da empresa contratada;
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços. A notificação deverá ocorrer com 30 dias de antecedência da data prevista para a interrupção dos serviços prestados e deverá determinar que:
  - A empresa contratada se obriga a aceitar eventual pedido de prazo adicional de 30 dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;
  - A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da CELCOIN.

## 21.6. Comunicação ao Bacen

A comunicação ao Bacen deve conter as seguintes informações:

O nome da empresa a ser contratada;

- Os serviços relevantes a serem contratados; e

- No caso de contratação no exterior, indicação dos locais onde os serviços serão prestados e os dados armazenados, processados e gerenciados.

O prazo para comunicação será de 10 dias, contados a partir da contratação dos serviços. Caso haja alterações contratuais que impliquem em modificação das informações, a comunicação ao Bacen deverá ocorrer em 10 dias contados da alteração contratual, salvo na hipótese prevista no item 18 “d”.

## 22. COMUNICAÇÃO AO BACEN

A comunicação ao Bacen deve conter as seguintes informações:

No tocante à continuidade dos serviços de pagamento prestados, a CELCOIN tem a responsabilidade de assegurar:

- O tratamento dos incidentes relevantes relacionados com o ambiente cibernético;
- Os procedimentos a serem seguidos no caso de interrupção de serviços 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 CELCOIN;
- Os cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados.
- O tratamento para mitigar os efeitos dos incidentes relevantes da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados;
- O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;
- A comunicação tempestiva ao Bacen das ocorrências de incidentes relevantes e das interrupções dos serviços, que configurem uma situação de crise pela CELCOIN, bem como das providências para o reinício das suas atividades.

A CELCOIN deverá instituir mecanismos de acompanhamento e de controle visando a assegurar a implementação e a efetividade desta Política, 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.

Os mecanismos de acompanhamento e controle deverão incluir a definição de processos, testes e trilhas de auditoria, bem como a definição de métricas e indicadores adequados e a identificação e a correção de eventuais deficiências.

## **23. REVISÃO E ATUALIZAÇÃO**

Esta Política será revista e atualizado, no mínimo, anualmente, ou quando da ocorrência de eventos considerados relevantes pela CELCOIN.

## **24. DISPOSIÇÕES GERAIS**

Esta Política entra em vigor na data de sua aprovação pela Diretoria e revoga quaisquer documentos em contrário às suas disposições.

Esta Política será documentado e mantido à disposição do Banco Central do Brasil pelo período em que estiver em vigor.

## Controle de Revisões e Atualizações

Versão	Referência	Data	Edição	Revisão	Aprovação
3.0	P-BRPSI-002	01/2023	Eduardo Francisco	Adam Nascimento	Diretoria