SOCRED

CRÉDITO NO QUE ACREDITAS

POLÍTICA
DE SEGURANÇA CIBERNÉTICA

Atualizada em 06/2026

POLÍTICA DE SEGURANÇA CIBERNÉTICA
Sumário

Sumário 2

1 OBJETIVO 5

2 PÚBLICO-ALVO 5

3 PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO 5

4 RESPONSABILIDADES 5

I. Diretor (Raimundo Nonato Nogueira da Costa): 5

II. Diretora Executiva (Nayara Nogueira da Costa): 5

5 DIRETRIZES DE SEGURANÇA CIBERNÉTICA 6

5.1 Classificação dos dados e das informações 6

5.2 Cenários de incidentes 7

5.3 Procedimentos e controles para prestadores de serviços 7

5.4 Avaliação da relevância dos incidentes 7

5.5 Cultura de Segurança Cibernética 8

5.6 Prestadores Críticos de Tecnologia 8

6 PROCEDIMENTOS E CONTROLES 8

6.1 Autenticação 8

6.2 Criptografia 9

6.3 Prevenção e detecção de intrusão 9

6.4 Prevenção de vazamento de informações 9

6.5 Detecção de vulnerabilidades 9

6.6 Proteção contra software malicioso 9

6.7 Mecanismos de rastreabilidade para informações sensíveis 9

6.8 Controles de acesso 9

6.8.1 Gestão de Certificados Digitais 10

6.8.2 Gestão de Chaves e Credenciais 10

6.9 Backup dos dados e das informações 10

6.10 Registro e controle dos efeitos de incidentes relevantes 10

6.11 Gestão de prestadores de serviço 11

6.12 Plano de ação e de resposta a incidentes 11

6.13 Divulgação de Incidentes Relevantes 12

6.14 Procedimento detalhado de identidade e acessos 12

6.15 Gestão de Vulnerabilidades e Testes 12
6.16 Inventário de Ativos 13
6.17 Operação SPI, SPB e RSFN 13
6.18 Uso de Inteligência Artificial 13
7 CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM 13
7.1 Abrangência 13
7.2 Avaliação da relevância do serviço a ser contratado 14
7.3 Avaliação da capacidade do potencial prestador de serviço 14
7.4 Contratação de serviços prestados no exterior 15
7.5 Cláusulas contratuais 15
7.6 Comunicação da contratação ao BACEN 16
8 CULTURA DE SEGURANÇA CIBERNÉTICA 17
9 RELATÓRIO ANUAL 17
9.2 Indicadores de Segurança Cibernética 17
10 DOCUMENTAÇÃO 18
11 GERENCIAMENTO CONTÍNUO DE RISCOS CIBERNETICO 18
11.1 INTRODUÇÃO 18
11.2 O OBJETIVO E DEFINIÇÕES 19
11.3 PRINCIPIOS E VALORES 19
11.4 CRITÉRIOS E PROCEDIMENTOS 20
GERÊNCIA 21
COLABORADORES E PRESTADORES DE SERVIÇOS 22
11.6 Declaração de Responsabilidade 22
11.7 Treinamento 23
11.8 SERVIÇOS DE COMPUTAÇÃO EM NUVEM 23
11.9 CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM 23
11.10 CONTRATOS COM PRESTADORES DE SERVIÇOS 24
11.11 AÇÕES DE PROTEÇÃO E PREVENÇÃO DE RISCOS CIBERNÉTICO 26
11.12 TRATAMENTO DE INCIDENTES 26

11.13 RELATÓRIO DE PLANO DE AÇÃO E RESPOSTA A INCIDENTES 27

11.14 DOCUMENTAÇÃO MÍNIMA A SER ARQUIVADA 28

11.15 CONSIDERAÇÕES FINAIS 28

12 DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA 28

13 COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO 28

14 VIGÊNCIA E REVISÃO 28

15 APROVAÇÃO DA POLÍTICA 28

POLÍTICA DE SEGURANÇA CIBERNÉTICA

1 OBJETIVO

Esta Política de Segurança Cibernética tem por objetivo definir princípios e diretrizes que permitam garantir a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela instituição, bem como orientar a implementação de procedimentos e controles para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

2 PÚBLICO-ALVO

Esta política aplica-se a todos os sócios, administradores, diretores e demais colaboradores da instituição, clientes, parceiros e prestadores de serviços a terceiros que tenham acesso aos dados da instituição ou aos sistemas informatizados por ela utilizados.

3 PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Os princípios que regem esta política são:

- **Confidencialidade:** garantir que a informação esteja acessível somente às pessoas autorizadas.
- **Integridade:** garantir a autenticidade da informação e dos seus métodos de processamento.
- **Disponibilidade:** garantir que a informação esteja disponível às pessoas autorizadas sempre que for necessário acessá-la.

4 RESPONSABILIDADES

Devido ao porte, o perfil de risco e o modelo de negócio da instituição ficam definidas as seguintes responsabilidades:

I. Diretor (Raimundo Nonato Nogueira da Costa):

- Aprovar a Política de Segurança Cibernética;
- Executar o Plano de Ação e de Resposta a Incidentes;
- Promover a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

II. Diretora Executiva (Nayara Nogueira da Costa):

- Realizar o registro e o controle dos efeitos de incidentes relevantes;
- Realizar periodicamente testes e varreduras para detecção de vulnerabilidades;
- Assegurar o acompanhamento dos mecanismos de cópia de segurança dos dados e das informações mantidos pela instituição e por seus prestadores críticos;
- Realizar a atividade de documentação referente à verificação de capacidade do

potencial prestador de serviço, das práticas de governança corporativa e da avaliação da relevância do serviço a ser contratado;
- Elaborar relatório anual sobre a implementação do Plano de Ação e de Resposta a Incidentes, tratada no item 14 desta política;
- Comunicar ao Banco Central do Brasil sobre a ocorrência de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela instituição, bem como as providências para o reinício das atividades;
- Comunicar ao Banco Central do Brasil sobre a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

A Diretoria deverá receber periodicamente informações relacionadas aos riscos cibernéticos, incidentes relevantes, vulnerabilidades identificadas, situação dos prestadores críticos de tecnologia e andamento dos planos de ação decorrentes de auditorias, testes ou avaliações de segurança.

5 DIRETRIZES DE SEGURANÇA CIBERNÉTICA

Esta política estabelece as seguintes diretrizes gerais:

- Atender às leis e normas que regulamentam as atividades da instituição;
- Assegurar a proteção das informações contra acessos, modificações, destruições ou divulgações não autorizadas;
- Assegurar que as informações sejam acessadas e utilizadas somente para as finalidades para as quais foram coletadas;
- Assegurar a adequada classificação dos dados e das informações relevantes para a operação da instituição;
- Estabelecer procedimentos e controles de segurança da informação para a prevenção, detecção e redução de riscos cibernéticos;
- Disseminar a cultura de segurança cibernética por meio da capacitação e avaliação dos colaboradores da instituição;
- Assegurar a aderência de terceiros relacionados aos negócios da instituição a esta política e a legislação e regulamentação aplicáveis.

5.1 Classificação dos dados e das informações

As informações sob responsabilidade da instituição serão classificadas considerando a relevância, sensibilidade, criticidade e grau de sigilo para o negócio e clientes, nos seguintes níveis:

- **Pública:** são informações que possuem caráter informativo geral e que são direcionadas ao público em geral;
- **Interna:** são informações destinadas ao uso interno da instituição e que estão disponíveis para todos os colaboradores da instituição;
- **Restrita:** são informações disponíveis apenas a colaboradores específicos da instituição, que as necessitem para exercer suas atribuições;
- **Confidencial:** são informações sigilosas de caráter estratégico para a instituição

e que estão disponíveis somente para a diretoria e pessoas por ela autorizadas.

5.2 Cenários de incidentes

Devem ser elaborados, no âmbito dos testes de continuidade de negócios, cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados pela instituição, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição, levando-se em consideração para a elaboração desses cenários a ausência de ativos humanos ou tecnológicos.

5.3 Procedimentos e controles para prestadores de serviços

Na elaboração de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros, considerando as características do serviço a ser prestado e níveis de complexidade, abrangência e precisão, deverão ser analisados cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados.

Uma vez identificados os possíveis cenários, serão analisados os controles voltados à prevenção e ao tratamento dos incidentes já utilizados pela prestadora, e, caso necessário, deverão ser estabelecidos com a respectiva prestadora de serviços outros procedimentos e controles de prevenção e tratamento dos incidentes a serem adotados, de forma a suprir as possíveis lacunas relativas à prevenção, detecção e redução da vulnerabilidade a incidentes relacionados com o ambiente cibernético.

São consideradas, para fins de aplicação do disposto nesta política, as empresas prestadoras de serviços a terceiros que tiverem acesso:

- Aos dados da instituição ou por ela controlados; ou
- Aos sistemas utilizados pela instituição; ou
- Aos ambientes físicos ou tecnológicos que possam ser utilizados para acessar os dados e sistemas da instituição.

5.4 Avaliação da relevância dos incidentes

Os parâmetros a serem utilizados na avaliação da relevância dos incidentes deverão considerar a frequência e o impacto dos cenários de incidentes que impliquem em danos ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição.

5.5 Cultura de Segurança Cibernética

A SOCRED promoverá a disseminação da cultura de segurança cibernética por meio de:

• Treinamentos periódicos para colaboradores;
• Capacitação obrigatória para novos colaboradores;
• Divulgação de orientações sobre boas práticas de segurança;
• Conscientização quanto à proteção de dados, sigilo bancário e prevenção a fraudes;
• Registro das ações de capacitação realizadas.

5.6 Prestadores Críticos de Tecnologia

A SOCRED manterá processo de identificação e monitoramento dos prestadores críticos de tecnologia, incluindo fornecedores responsáveis por processamento de dados, armazenamento, computação em nuvem, core bancário, ERP, mensageria financeira e demais serviços relevantes para a continuidade operacional.

A avaliação considerará aspectos relacionados à segurança da informação, continuidade de negócios, gestão de incidentes, disponibilidade dos serviços e conformidade regulatória.

Consideram-se prestadores críticos aqueles cuja indisponibilidade possa impactar a continuidade operacional, a prestação de serviços financeiros ou o cumprimento de obrigações regulatórias da instituição.

6 PROCEDIMENTOS E CONTROLES

A instituição adota os seguintes procedimentos e controles para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético:

6.1 Autenticação

Para garantir a segurança dos acessos a instituição adota regras de autenticação para o sistema operacional e banco de dados, os quais utiliza mecanismos de autenticação e armazenamento seguro de credenciais compatíveis com os requisitos de segurança da instituição. Sendo que o chamado de consulta do login do usuário pelo sistema é feito em ambiente criptografado por chaves SSL.

Acessos com a exigência de autenticação:

- Sistema de e-mail;
- Consulta a base de dados (em todos os canais);
- Sistema ERP;
- Diretórios e arquivos na rede de computadores.

A senha de acesso ao sistema utiliza caracteres alfanuméricos e especiais, é composta de 8 (oito) a 10 (dez) dígitos. As credenciais de autenticação são protegidas por mecanismos criptográficos compatíveis com as boas práticas de segurança da informação e com os requisitos de segurança adotados pela instituição.

A concessão de acessos observará os princípios da identificação individual, menor privilégio, necessidade de conhecimento e segregação de funções.

6.2 Criptografia

O sistema de comunicação e transmissão de dados da instituição é criptografado utilizando chave SSL em seu ambiente, as senhas e logins de acesso são criptografadas.

6.3 Prevenção e detecção de intrusão

A instituição utiliza soluções corporativas de proteção de rede, prevenção e detecção de intrusões, monitoradas por equipes internas ou prestadores especializados, capazes de registrar eventos de segurança e auxiliar na identificação de acessos indevidos e tentativas de ataque.

6.4 Prevenção de vazamento de informações

O Banco de dados da instituição é mantido em rede interna apartado do ambiente do sistema operacional, e mantido atrás de camadas de segurança, com os mecanismos de monitoramento e proteção mantendo o sistema operacional seguro e estável. Ao sinal de indício de instabilidade ou tentativa de comprometer algo no sistema, recebemos um alerta que prontamente é atendido na ocorrência.

6.5 Detecção de vulnerabilidades

A SOCRED adota mecanismos de monitoramento e gestão de vulnerabilidades destinados à identificação, correção e mitigação de falhas de segurança em seus ambientes tecnológicos, próprios ou terceirizados. As vulnerabilidades identificadas deverão ser avaliadas e tratadas de acordo com sua criticidade.

6.6 Proteção contra software malicioso

A instituição utiliza soluções corporativas de proteção contra softwares maliciosos, mecanismos de atualização de segurança e sistemas operacionais mantidos e atualizados, compatíveis com os requisitos de segurança da informação e continuidade dos negócios..

6.7 Mecanismos de rastreabilidade para informações sensíveis

Os sistemas contêm locais fixos onde são imputados os dados originados da instituição financeira, esses dados competem única e exclusivamente na origem, baseado nos produtos e políticas da instituição. Locais onde estão armazenados estão contidos em relatórios de uso interno.

6.8 Controles de acesso

O sistema dispõe de mecanismos de log, e fornece rastreabilidade dos acessos. As

telas de sistema são segregadas de acordo com as funções estabelecidas aos usuários.

Os acessos deverão ser revisados periodicamente, contemplando usuários internos, terceiros e acessos privilegiados.

Os acessos não mais necessários deverão ser revogados tempestivamente.

Sempre que tecnicamente possível serão utilizados mecanismos de autenticação multifator para sistemas críticos e acessos administrativos.

6.8.1 Gestão de Certificados Digitais

A SOCRED adotará controles para emissão, armazenamento, utilização, renovação, substituição e revogação de certificados digitais utilizados em seus serviços críticos, incluindo aqueles empregados na comunicação com o Sistema Financeiro Nacional.

6.8.2 Gestão de Chaves e Credenciais

Credenciais, senhas, chaves criptográficas e certificados digitais deverão ser protegidos contra acesso não autorizado, observando critérios de armazenamento seguro, controle de acesso e rastreabilidade.

6.9 Backup dos dados e das informações

A SOCRED manterá mecanismos de cópia de segurança compatíveis com a criticidade de seus serviços, contemplando procedimentos de armazenamento, recuperação e testes periódicos de restauração.

Os ambientes críticos deverão possuir mecanismos de redundância e recuperação adequados para assegurar a continuidade das operações.

A efetividade dos mecanismos de recuperação deverá ser validada periodicamente por meio de testes documentados de restauração.

6.10 Registro e controle dos efeitos de incidentes relevantes

Os incidentes são registrados com o seu devido código de prioridade conforme definido no Plano de Ação e Resposta a Incidentes, onde é descrito a forma como devem ser registrados e tratados os incidentes de segurança, sendo que nos processos e ocorrências, caso os responsáveis verifiquem grau de importância, devem notificar responsáveis e envolvidos, e observar outros itens obrigatórios ou de interesse, além de atualizar rotinas e processos de documentos como a própria política, manuais e outros que a instituição defina como necessário.

Os incidentes deverão ser classificados conforme seu impacto sobre a confidencialidade, integridade e disponibilidade das informações, podendo ser categorizados conforme critérios internos de severidade.

Incidentes considerados relevantes serão comunicados tempestivamente à Diretoria e, quando aplicável, aos órgãos reguladores competentes.

6.11 Gestão de prestadores de serviço

Os contratos com prestadores de serviço deverão conter cláusulas de confidencialidade e responsabilidades entre as partes, assim como cláusulas que garantam que os profissionais das empresas prestadoras de serviços a terceiros:

- Tenham conhecimento e cumpram esta política;
- Zelem e protejam o sigilo das informações da instituição;
- Cumpram as normas legais que regulamentam a propriedade intelectual e a proteção de dados e a normas vigentes relacionadas à segurança cibernética e afins do Banco Central do Brasil;
- Utilizem os dados da instituição ou os sistemas por ela utilizados, bem como os ambientes físico e tecnológico da instituição, apenas para as finalidades objeto do contrato de prestação de serviço;
- Notifiquem imediatamente qualquer violação desta Política ou outras normas.

6.12 Plano de ação e de resposta a incidentes

A presente política institui o Plano de Ação e de Resposta a Incidentes com os seguintes objetivos:

- Identificar os incidentes de segurança;
- Registrar os eventos que acarretaram problemas de segurança/continuidade;
- Direcionar medidas paliativas a incidentes ocorridos;
- Criar evidências e registros para medidas corretivas;
- Acionar o plano de continuidade dos negócios;
- Reportar os incidentes de segurança;
- Adotar iniciativas para compartilhamento de informações sobre incidentes relevantes com outras instituições.

Esse plano abordará detalhadamente os cenários de incidentes a serem avaliados nos testes de continuidade de negócios, considerando a avaliação de risco dos incidentes por níveis de impacto nos negócios, sendo esses níveis estipulados em Gravíssimo, Grave, Médio, Baixo e Muito Baixo.

Por meio da identificação do nível de impacto do incidente será sequenciado o processo para o devido encaminhamento aos responsáveis para tratamento, conclusão e registro. A instituição definiu um relatório de Incidente de Risco Cibernético (RIRC) de forma a registrar, acompanhar e simular cenários de impacto dos incidentes de segurança.

No plano a instituição elencou os serviços primordiais e os possíveis cenários que acarretariam prejuízo nos ou parada dos negócios. Para tanto, foram mapeados

cenários que apresentaram risco de interrupção a serem considerados para os testes de efetividade do plano de continuidade dos negócios, sendo estes:

- Interrupção de fornecimento de link de dados;
- Sinistro em servidor interno de dados;
- Interrupção do acesso ao Banco de Dados (Sistema Operacional na nuvem).

O plano deverá contemplar critérios para identificação, contenção, mitigação, recuperação e comunicação de incidentes, incluindo situações classificadas como crise operacional ou cibernética.

Será utilizado o relatório de implementação do plano de ação anual, de forma a evidenciar necessidades de revisões assim como simular e registrar os testes de continuidade dos negócios nos cenários definidos pela administração.

Registra-se que o Plano de Ação e de Resposta a Incidentes, Plano de Continuidade dos Negócios e Relatórios de Registro, Teste e Acompanhamento complementam e integram a presente política.

6.13 Divulgação de Incidentes Relevantes

Visando maior transparência bem como a busca pelas melhores práticas de mercado a instituição diante da ocorrência de incidentes cibernéticos relevantes buscará a adequada divulgação em sítio na internet, disponibilizando canal para solicitação de maior detalhamento para interessados.

6.14 Procedimento detalhado de identidade e acessos

A SOCRED adotará controles para garantir que os acessos aos sistemas, informações e ambientes tecnológicos sejam concedidos de acordo com as atribuições de cada usuário.

Os acessos deverão observar:

• Identificação individual do usuário;
• Segregação de funções;
• Revisão periódica dos perfis de acesso;
• Revogação imediata de acessos desnecessários;
• Registro dos acessos realizados;
• Controle de alterações de perfis e permissões.

Os sistemas críticos deverão permitir a rastreabilidade dos acessos e das operações realizadas pelos usuários.

6.15 Gestão de Vulnerabilidades e Testes

A SOCRED realizará avaliações periódicas de vulnerabilidades e testes de segurança compatíveis com seu porte, perfil de risco e ambiente tecnológico, incluindo testes de

vulnerabilidade, testes de invasão (pentest), quando aplicável, e acompanhamento dos planos de correção das vulnerabilidades identificadas.

6.16 Inventário de Ativos

A SOCRED manterá inventário atualizado dos ativos tecnológicos relevantes, incluindo hardware, software, sistemas, aplicações, certificados digitais e demais recursos necessários à execução de suas atividades, de forma a apoiar os processos de gestão de riscos, continuidade de negócios e segurança cibernética

6.17 Operação SPI, SPB e RSFN

Para os ambientes relacionados ao SPI, SPB e RSFN, a SOCRED adotará controles específicos de segurança, incluindo gestão de certificados digitais, segregação lógica dos ambientes, rastreabilidade dos acessos, controle de usuários privilegiados, monitoramento dos acessos administrativos e procedimentos de renovação, substituição e revogação de certificados.

6.18 Uso de Inteligência Artificial

O uso de ferramentas de Inteligência Artificial deverá observar os princípios de confidencialidade, integridade e disponibilidade das informações. É vedada a inserção de informações protegidas por sigilo bancário, dados pessoais sensíveis ou informações estratégicas da instituição em plataformas não homologadas pela SOCRED. Novas soluções baseadas em Inteligência Artificial deverão ser previamente avaliadas sob a ótica de riscos e segurança da informação.

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

A instituição adotará procedimentos e práticas de governança corporativa e de gestão que serão aplicadas previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, levando-se em consideração a avaliação da relevância do serviço a ser contratado, dos riscos a que esteja exposta a instituição, bem como da capacidade do potencial prestador de serviço em realizar as atividades conforme a legislação e regulamentação aplicáveis.

7.1 Abrangência

Os procedimentos e práticas serão aplicados previamente à contratação de serviços de processamento e armazenamento de dados e de serviços de computação em nuvem.

Os serviços de computação em nuvem, prestados sob demanda e de maneira virtual, compreendem a disponibilidade de ao menos um dos serviços abaixo:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e

outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;

- Implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;
- Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

7.2 Avaliação da relevância do serviço a ser contratado

A avaliação prévia da relevância do serviço de processamento e armazenamento de dados e de computação em nuvem a ser contratado levará em consideração:

- A criticidade do serviço;
- A sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado;
- A classificação dos dados e das informações quanto à relevância.

7.3 Avaliação da capacidade do potencial prestador de serviço

A instituição avaliará previamente, como critérios de decisão para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, a capacidade do potencial prestador de serviço em assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso da instituição aos dados e às informações a serem processadas ou armazenadas;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas;
- A sua aderência às certificações exigidas por lei e pela instituição para a prestação do serviço a ser contratado;
- O acesso da instituição 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 instituição 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 instituição;
- A adoção de controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos executados por meio da internet, implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviço.

A avaliação da capacidade dos prestadores deverá considerar mecanismos relacionados à confidencialidade, integridade, disponibilidade, recuperação de dados, continuidade de negócios, gestão de incidentes e segurança dos ambientes utilizados.

7.4 Contratação de serviços prestados no exterior

De modo complementar ao item 7.3, no caso de contratação de serviços prestados no exterior, a instituição observará previamente os seguintes critérios:

- A existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
- Se a prestação dos serviços no exterior não causa prejuízos ao regular funcionamento da instituição e nem embaraço à atuação do Banco Central do Brasil;
- A definição dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- A 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.

No caso de não existir convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados, a instituição solicitará ao Banco Central do Brasil, no prazo de 60 (sessenta) dias anteriores à contratação, autorização para a contratação do serviço.

7.5 Cláusulas contratuais

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

- A indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;
- A obrigatoriedade, em caso de extinção do contrato, de:
  a) Transferência dos dados ao novo prestador de serviços ou à instituição contratante;
  b) Exclusão dos dados pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos;
- O acesso da instituição contratante a:
  a) Informações fornecidas pela empresa contratada, visando a verificar o cumprimento dessas obrigações;

b) Informações relativas às certificações e aos relatórios de auditoria especializada;

c) Informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

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

Os contratos devem prever, ainda, cláusulas específicas para o caso de decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil:

- A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados no inciso VII do caput, que estejam em poder da empresa contratada;
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

  a) A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;

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

7.6 Comunicação da contratação ao BACEN

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada ao Banco Central do Brasil, devendo a comunicação conter as seguintes informações:

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

A referida comunicação deve ser realizada, no máximo, até 10 (dez) dias após a contratação dos serviços e as alterações contratuais que impliquem modificação dessas informações devem ser comunicadas ao Banco Central do Brasil, no máximo, até 10 (dez) dias após a alteração contratual.

8 CULTURA DE SEGURANÇA CIBERNÉTICA

A instituição adotará os seguintes mecanismos para a disseminação da cultura de segurança cibernética:

- Promover a implementação de programas de capacitação e de avaliação periódica de todos os colaboradores;
- Prestar informações aos usuários finais sobre precauções na utilização de produtos e serviços oferecidos;
- Comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

A participação dos colaboradores nos treinamentos e ações de conscientização deverá ser registrada e mantida como evidência dos programas de capacitação promovidos pela instituição.

9 RELATÓRIO ANUAL

Anualmente, a instituição elaborará relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes, tendo como data-base o dia 31 (trinta e um) de dezembro de cada ano.

O relatório deverá ser submetido a Diretoria da instituição até 31 (trinta e um) de março do ano seguinte ao da data-base, devendo abordar:

- A efetividade da implementação das ações desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes desta política;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizadas na prevenção e na resposta a incidentes;
- Os incidentes relevantes relacionados com o ambiente cibernético, ocorridos no período;
- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes de segurança.

9.1. Indicadores de Segurança Cibernética

A SOCRED acompanhará periodicamente indicadores relacionados à segurança cibernética, podendo incluir:

• Quantidade de incidentes cibernéticos;
• Quantidade de indisponibilidades relevantes;

• Disponibilidade dos serviços críticos;
• Quantidade de vulnerabilidades identificadas;
• Quantidade de acessos revisados;
• Situação dos planos de ação relacionados à segurança cibernética.

10 DOCUMENTAÇÃO

Devem ficar à disposição do Banco Central do Brasil, pelo prazo de 5 (cinco) anos:

- O documento relativo à política de segurança cibernética;
- O documento relativo ao plano de ação e de resposta a incidentes;
- Os relatórios anuais sobre a implementação do plano de ação e de resposta a incidentes;
- A documentação sobre os procedimentos e práticas de governança corporativa e de gestão e a avaliação da capacidade do potencial prestador de serviço;
- A documentação referente à contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, prestados no exterior;
- Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, contado o prazo a partir da extinção do contrato;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle para implementação e efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, contado o prazo referido no caput a partir da implementação dos citados mecanismos.

11 GERENCIAMENTO CONTÍNUO DE RISCOS CIBERNETICO

Será parte integrante da Plano de Gerenciamento de Riscos.

11.1 INTRODUÇÃO

A Estrutura Simplificada de Gerenciamento Contínuo de Riscos Cibernéticos da SOCRED, tem por finalidade definir diretrizes para efetivar e para manutenção das estratégias, rotinas e procedimentos de gerenciamento de riscos cibernético.
A SOCRED mantém Estrutura Simplificada De Gerenciamento Contínuo De Riscos em atendimento a Resolução nº 4.557/17 e Resolução 4.606/17 com objetivo de identificar, mensurar, avaliar, monitorar, reportar, controlar e mitigar O RISCO CIBERNETICO que a instituição esteja exposta de maneira relevante, considerando:

- O modelo de negócios, com a natureza das operações, complexidade dos produtos e serviços, das atividades e dos processos da SOCRED;
- A dimensão e à relevância da exposição aos riscos, segundo critérios definidos pela SOCRED.
- Adequada ao Perfil de riscos da SOCRED.

A política atende as exigências legais e os controles estabelecidos são entendidos como oportunidade de melhoria nos padrões éticos e na transparência das informações.

POLÍTICA DE SEGURANÇA CIBERNÉTICA

A SOCRED mantém estrutura de TI que assegura a integridade, a segurança e a disponibilidade dos dados relativos ao gerenciamento de riscos.

A SOCRED mantém a política de continuidade de negócios que esteja exposta de maneira relevante. Os modelos e os procedimentos internos asseguram as operações realizadas através de procedimentos e pessoal qualificado para a função. Todas as análises e procedimentos de risco serão reportados a Diretoria. A SOCRED deverá manter atualizado o Relatório Gerencial versando sobre o desempenho da estrutura simplificada de gerenciamento de risco cibernético. A documentação relativa à estrutura de gerenciamento de riscos cibernético ficará à disposição do Banco Central do Brasil por cinco anos.

11.2 O OBJETIVO E DEFINIÇÕES.

O objetivo desta Política é orientar a administração da SOCRED na gestão da segurança da informação e cibernética, demonstrando o compromisso com a proteção das informações corporativas e demais ativos de informação, destinados a garantir a confidencialidade, integridade e disponibilidade das informações.

Para atingir o objetivo são determinados procedimentos internos destinados a minimizar a ocorrência de riscos cibernéticos e para identificar violações de segurança cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos.

A SOCRED garante a confidencialidade, integridade e disponibilidade da informação em todo o seu ciclo de vida: produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte. Para esclarecimentos dessa política são definidos:

a) Segurança cibernética: é um conjunto de práticas que protege informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a internet e telefones celulares;
b) Ativos de informações: são todas as informações geradas ou desenvolvidas para operação da SOCRED, e podem estar presentes em diversas formas, tais como: arquivos digitais, equipamentos, mídias externas, documentos impressos, sistemas, dispositivos móveis, bancos de dados e conversas;
c) Incidentes: qualquer ocorrência que não é parte padrão da operação de um serviço e que pode causar uma indisponibilidade, redução na qualidade dele, perda de integridade ou confidencialidade das informações;
d) Risco cibernético: ameaça à confidencialidade, integridade e disponibilidade das informações.

11.3 PRINCIPIOS E VALORES

A SOCRED possui como princípios seu compromisso com a transparência e o respeito nas relações para com seus funcionários, usuários dos serviços financeiros.

As informações dos usuários de serviços financeiros são guardadas de acordo com padrões de confidencialidade e segurança, sendo compartilhados à terceiros, nos termos da lei, desde que necessários para a execução de serviços/operações contratadas e sob o dever de proteção de dados e confidencialidade dos mesmos.

Assim, como princípios e valores que norteiam essa política de Risco Cibernético são:

a) Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

b) Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas (acidentais ou propositais);
c) Disponibilidade: garantir que as informações estejam disponíveis às pessoas autorizadas somente para executar o tratamento necessário.

11.4 CRITÉRIOS E PROCEDIMENTOS

A SOCRED adotará critérios e procedimentos compatíveis com seu porte, perfil de risco, modelo de negócios e complexidade operacional, visando prevenir, detectar, responder e mitigar riscos cibernéticos.

Para tanto, serão observados, no mínimo, os seguintes controles:

a) Gestão de acessos e identidades, observando os princípios da identificação individual, menor privilégio, segregação de funções e revisão periódica dos acessos concedidos;

b) Gestão de vulnerabilidades, incluindo avaliações periódicas, acompanhamento de correções e testes de segurança compatíveis com o ambiente tecnológico da instituição;

c) Gestão de ativos tecnológicos, mantendo inventário atualizado de hardware, software, aplicações críticas, certificados digitais e demais recursos necessários à operação;

d) Gestão de certificados digitais, contemplando procedimentos de emissão, utilização, armazenamento, renovação, substituição e revogação;

e) Monitoramento dos ambientes tecnológicos e dos serviços críticos utilizados pela instituição;

f) Controles de segurança aplicáveis aos ambientes relacionados ao SPI, SPB, RSFN e demais infraestruturas críticas do Sistema Financeiro Nacional;

g) Gestão de prestadores críticos de tecnologia, considerando aspectos relacionados à segurança da informação, continuidade de negócios, gestão de incidentes e conformidade regulatória;

h) Adoção de mecanismos de cópia de segurança, redundância e recuperação de dados compatíveis com a criticidade dos serviços;

i) Avaliação periódica dos riscos decorrentes da utilização de novas tecnologias, incluindo serviços em nuvem, APIs e soluções baseadas em Inteligência Artificial;

j) Implementação de ações de conscientização e treinamento voltadas à disseminação da cultura de segurança cibernética.

Os controles previstos neste item deverão ser revisados periodicamente e sempre que ocorrerem alterações relevantes no ambiente operacional, tecnológico ou regulatório da instituição.

11.5 ÁREAS ENVOLVIDAS / RESPONSABILIDADES

A Diretoria é responsável pela política de Segurança Cibernética, devendo ser revisada e atualizada de maneira que demonstre e identifique preventivamente a existência de vulnerabilidades que possam expor a SOCRED a riscos, considerados incompatíveis com os níveis de riscos aceitáveis, para que as ações sejam tomadas para reduzir essa exposição.

A Diretoria, também continuamente mantém a correção de eventuais deficiências da estrutura simplificada de gerenciamento de riscos que possam ser identificadas, assegura a observância por todos na SOCRED. Compete a Diretoria no mínimo a cada ano aprovar e revisar as políticas e estratégias de gerenciamento de riscos operacional.

Cabe a diretoria prover recursos para a implementação, manutenção e melhoria da gestão de segurança cibernética; promovendo a disseminação da cultura de gerenciamento de riscos por todos os participantes da SOCRED.

Todo componente da estrutura organizacional da SOCRED, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações e deve cumprir as determinações desta política, normas e padrões de segurança cibernética.

A SOCRED entende que é importante que cada colaborador deve focar na conformidade com as normas, leis, padrões e/ou procedimentos internos ou externos. Tudo isso com o propósito de mitigar as diversas vulnerabilidades às quais a SOCRED está sujeita.

GERÊNCIA

As gerências têm como responsabilidade:

a) Assegurar que todos da equipe tenham acesso, conhecimento e implementação pratica desta política e demais normas e padrões de segurança de cibernética;
b) Assegurar que o acesso a dados e informações pela equipe seja somente o necessário ao desempenho de suas funções, atribuições e para cumprimento das operações e atividades da SOCRED;

c) Avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe, garantindo a confidencialidade, integridade e disponibilidade das informações.
d) Designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;
e) Identificar com a equipe técnica as violações de segurança cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos;

Ainda que seja com o suporte de área técnica a Gerência será responsável em:
a) Desenvolver e estabelecer programas de conscientização e divulgação da política de segurança cibernética;
b) Conduzir o processo de gestão de riscos de segurança cibernética;
c) Conduzir a gestão de incidentes de segurança cibernética, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;
d) Conduzir a definição controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas;
e) Propor projetos e iniciativas para melhoria do nível de segurança das informações da SOCRED.

COLABORADORES E PRESTADORES DE SERVIÇOS

Todos os colaboradores e prestadores que tenham qualquer acesso cibernético e as informações da SOCRED será responsável:
a) Utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de segurança cibernética.
b) Utilizar os dados pessoais de forma licita e somente para o que foi aprovado a sua utilização e não armazenar além do determinado nos procedimentos operacionais da SOCRED.
c) Notificar a área segurança da informação e cibernética os incidentes de segurança que venha a tomar conhecimento e as violações desta política de segurança cibernética;

11.6 Declaração de Responsabilidade

Os colaboradores e prestadores de serviços diretamente devem aderir formalmente a um termo comprometendo-se a agir de acordo com a Política de Segurança Cibernética.

Seguindo as boas práticas, gradualmente deverá implementar aos contratos firmados com prestadores que tenham acesso cibernético e as informações da SOCRED cláusula que assegure a confidencialidade das informações protegidas por sigilo e pela legislação e regulamentação vigentes.

11.7 Treinamento

A SOCRED deve estabelecer um programa de treinamento e conscientização em Segurança Cibernética à garantia dos objetivos e diretrizes definidos nesta Política a fim de apresentar às necessidades e responsabilidades específicas de cada colaborador.

A SOCRED em seus treinamentos a colaboradores e/ou integrações a novos colaboradores deverá conscientizar que todas as ações, sistemas, serviços, dados, informações disponíveis não devem ser interpretadas como sendo de uso pessoal, portanto, todos devem ter ciência de que o uso está sujeito à monitoramento periódico, inclusive em equipamentos pessoais acessados durante o expediente, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pelo departamento de TI, gestores ou por prestador de serviços externo.

11.8 SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Os serviços de computação em nuvem abrangem:

a) Empregar de recursos computacionais dos prestadores de serviços em casos de implantação, execução de aplicativos adquiridos ou desenvolvidos pela SOCRED;
b) Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos que permitam a SOCRED implantar e executar softwares, que podem incluir sistemas operacionais e aplicativos internos ou adquiridos;
c) Usar de recursos computacionais do próprio prestador de serviços para execução por meio de internet dos aplicativos implantados ou desenvolvidos.

Na gestão dos serviços contratados devem ser avaliados a confiabilidade, integridade, disponibilidade, segurança e sigilo das informações, os recursos utilizados, bem como o cumprimento da legislação vigente.

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

A computação em nuvem é uma forma de contratação de serviços de terceiros, e esses prestadores de serviços de processamento e armazenamento de dados representam um risco de cIbersegurança para a SOCRED, sendo necessário cuidados em casos de identificação de ameaças.

Na contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior devem ser considerados os seguintes requisitos à empresa contratada:

a) Ter Política de Segurança Cibernética e plano de continuidade de negócios – PCN;
b) Manter registro e autorização em caso de mudanças ou alterações de serviços ou sistemas; e
c) Ter relatórios de controles e gestão de incidentes.

A SOCRED continuamente verifica a capacidade potencial do prestador de serviços de processamento e armazenamento de dados e de computação em nuvem a fim de assegurar o cumprimento da legislação em vigor, permissão de acessos da SOCRED aos dados e as informações que serão processadas ou armazenadas.

O prestador de serviços de processamento e armazenamento de dados e de computação em nuvem deve manter a confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas e armazenadas.

A SOCRED deverá ter acesso aos relatórios de auditoria contratada pelo prestador de serviço e fornecimento de informações e de recursos de gestão adequados aos monitoramentos dos serviços as serem prestados.

Os prestadores de serviços relevantes serão avaliados considerando a criticidade do tipo de serviços a ser prestado, bem como a sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas.

Ainda, devem ser verificadas a adoção de controles que reduzam eventuais vulnerabilidades na liberação de novas versões de aplicativos no caso de serem executados pela internet.

11.10 CONTRATOS COM PRESTADORES DE SERVIÇOS

Os contratos firmados com as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever a indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados que poderão ser armazenados, processados e gerenciados, bem como adoção de medidas de segurança para transmissão de armazenamento de dados.

Enquanto o contrato estiver vigente, deve prever a manutenção da segregação dos dados e dos controles de acessos para proteção das informações dos usuários dos serviços da SOCRED.

A empresa contratada deverá notificar a SOCRED sobre a subcontratação de serviços relevantes para a SOCRED.

A SOCRED deverá ter acesso às informações fornecidas pelas empresas contratadas visando verificar o cumprimento da indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados que poderão ser armazenados, processados e gerenciados, bem como adoção de medidas de segurança para transmissão de armazenamento de dados.

A empresa prestadora de serviço deverá disponibilizar a SOCRED o acesso as informações relativas ao relatório de auditoria especializada contratada pelo prestador de serviço e recursos de gestão adequadas ao monitoramento dos serviços contratados.

Os contratos devem prever ainda permissão de acesso ao Banco Central do Brasil – BCB nas seguintes informações;

a) Contratos e aos acordos firmados para a prestação de serviços;
b) Documentação e às informações referentes aos serviços prestados;
c) Dados armazenados e às informações sobre seus processamentos;
d) Cópias de segurança dos dados e das informações;
e) Códigos de acesso aos dados e às informações;
f) Adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e
g) Obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

O contrato mencionado na alínea “a” deve prever, para o caso da decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil:

a) A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados na alínea “g” do caput, que estejam em poder da empresa contratada; e

b) A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

b.1) a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;

b.2) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

11.11 AÇÕES DE PROTEÇÃO E PREVENÇÃO DE RISCOS CIBERNÉTICO

As ações de proteção e prevenção da SOCRED a fim de manter funcionamento e efetividade da segurança cibernética seguem os seguintes requisitos:

a) Manter relatório de inventários de hardware e software;

b) Verificar com frequência se há na SOCRED computadores não autorizados ou software não licenciado;

c) Manter os sistemas operacionais e software atualizados;

d) Realizar avaliações periódicas de vulnerabilidades e testes de segurança compatíveis com o porte, perfil de risco e ambiente tecnológico da instituição;

e) Fazer análises de vulnerabilidade na estrutura tecnológica da SOCRED frequentemente ou em situações que houver mudança significativas;

f) Fazer teste do plano de resposta a incidentes com simulação de cenários. A SOCRED realiza testes de segurança no seu sistema de segurança da informação e proteção de dados, dentre as medidas, incluem-se: Verificação dos logs dos colaboradores; Alteração periódica de senha de acesso dos Colaboradores; e segregação de acessos;

g) A SOCRED deverá solicitar para os fornecedores testes e eficácia dos processos utilizados para evitar e revelar as principais vulnerabilidades dos sistemas que estão sob a responsabilidades deles, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real;

11.12 TRATAMENTO DE INCIDENTES

Os incidentes são interrupções de sistema tecnológico não planejado que afetam os

negócios da SOCRED e podem acontecer nas seguintes situações:

a) Queda de energia;
b) Falha de um elemento de conexão ou servidor fora do ar;
c) Ausência de conexão com a internet;
d) Indisponibilidade de acesso a SOCRED.
e) Indícios ou ocorrências com perda, roubo ou vazamento de dados,
f) Terrorismo e ataques cibernéticos;

As ocorrências de incidentes devem ser avaliadas em relação à gravidade da situação, os motivos que levaram aos acontecimentos desses incidentes e as consequências para os negócios da SOCRED.

A SOCRED deverá realizar as seguintes ações após a avaliação dos incidentes:

a) Avaliar o impacto do incidente na SOCRED;
b) Redirecionar os contatos como as linhas de telefones para os celulares, instruir o provedor de telefonia a desviar linhas de dados, entre outros;
c) Avaliar a relevância, em caso de sabotagem ou terrorismo a fim de decidir pelo registro de boletim de ocorrência ou outras providencias caso seja necessário;
d) Comunicar tempestivamente ao Banco Central do Brasil – BCB as ocorrências de incidentes relevantes e as interrupções de serviços relevantes que configurem uma situação de crise na SOCRED.

Após o incidente ter sido resolvido com a contingência da segurança cibernética e demais equipes chaves notificados, as áreas devem verificar se os dados estão faltando ou foram corrompidos ou outros problemas.

Caso seja identificado que a SOCRED perdeu informações ou dados, so dirigentes com funções executivas e equipe de contingência da SOCRED devem ser informados imediatamente e na retomada dos processos deverão ser definidos ações que incluem a análise procedimentos para que a SOCRED possa operar normalmente, bem como reconstrução de eventuais sistemas e mudanças e medidas de prevenção.

11.13 RELATÓRIO DE PLANO DE AÇÃO E RESPOSTA A INCIDENTES

A SOCRED deverá emitir anualmente o relatório de implementação de plano de ação e respostas a incidentes. Os referidos relatórios devem ser aprovados pelos Diretores em função Executiva responsável pela segurança cibernética.

O relatório deverá ser emitido com data base de 31 de dezembro e conter, no mínimo, as seguintes informações:

a) Resumo dos resultados alcançados na implementação de rotinas, procedimentos e tecnologias utilizados na prevenção e na resposta a incidentes;

b) As ocorrências de incidentes relevantes ocorrido no período relacionado referente ao ambiente cibernético;

11.14 DOCUMENTAÇÃO MÍNIMA A SER ARQUIVADA

Devem ficar à disposição do Banco Central do Brasil – BCB:

a) A presente Política;
b) A ata da diretoria com a aprovação da política;
c) Documento relativo ao plano de ação e de resposta a incidentes;
d) Relatório anual e a documentação sobre os procedimentos;
e) Documentação que trata no caso de serviços prestados no exterior;
f) Os contratos de prestação de serviços relevantes de processamento,

11.15 CONSIDERAÇÕES FINAIS

Essa Política será revisada anualmente ou quando mudanças significativas exigirem.

12 DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Para divulgação desta política a instituição adotará as seguintes ações:

- Divulgação a todos os colaboradores da instituição e às empresas prestadoras de serviços a terceiros, de forma acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.
- Divulgação ao público, na página da instituição na internet, do resumo contendo as linhas gerais desta política.

13 COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

Ao aprovar esta Política de Segurança Cibernética, a Diretoria da instituição firma um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança cibernética, buscando sempre se manter em conformidade com as normas e regulamentos aplicáveis, sendo guiada pelos princípios, diretrizes e práticas aqui adotadas para assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou dos sistemas de informação por ela utilizados.

14 VIGÊNCIA E REVISÃO

Esta política terá vigência a partir da data de aprovação pela Diretoria, e será revisada e documentada anualmente ou a qualquer momento para se adequar a alterações regulatórias ou outras obrigações legais.

15 APROVAÇÃO DA POLÍTICA

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Esta política foi aprovada pela Diretoria em 09/06/2026, conforme Ata em anexo.

POLÍTICA DE SEGURANÇA CIBERNÉTICA

RIRC – Relatório de Incidente de Risco Cibernético ANUAL

RIRC Nº ____/2022

CÓDIGO DE IMPACTO:	( ) Gravíssimo ( ) Grave ( ) Médio ( ) Baixo ( ) Muito Baixo
Descrição:	
Período em que ocorreu o Incidente	Data Início:
	Data Fim:
Tipo de Impacto (s):	( ) Confidencialidade ( ) Integridade ( ) Disponibilidade
Origem da Ocorrência:	
Responsáveis Comunicados:	

Detalhamento do Incidente

<informar a categoria do incidente. Ex.: Alteração não planejada, Ataque DDoS, Não Conformidade com a PSI, etc>

<descrever o que ocorreu, extensão e impactos do incidente, bem como detalhar as causas do incidente, áreas envolvidas na investigação do incidente, etc>

Tratamento do Incidente

<descrever ações executadas para contenção e/ou contorno do problema/incidente, equipes/pessoas envolvidas. Atentar ao fato de que determinadas ações de contenção/contorno podem demandar sua prévia comunicação.

Análise e Encerramento do Incidente

<descrever se necessárias outras ações e recursos necessários para finalizar o tratamento do incidente e/ou para evitar que o incidente volte a ocorrer, informando, se possível, prazos e responsáveis para execução.> <lições aprendidas>

<informar identificador do chamado/problema vinculado ao incidente, se houver>

Considerar também a necessidade de:

- *reversão da solução de controle/contorno*
- *implementação de uma correção para a causa-raiz do problema;*

- *implantação de um novo serviço/sistema;*
- *substituição do ativo/sistema afetado;*

<Informar conclusões devidas caso teste de estresse e futuras alterações>

Acionamento do Plano de Continuidade

□ Sim

□ Não

Reporte aos Órgãos de Controle/Registro

□ BACEN

□ ABSCM

Assinatura dos Envolvidos