



Política Segurança da Informação e Risco Cibernético



1. Objetivo

Esta Política tem por objetivo definir as diretrizes referentes à Segurança da Informação e Risco Cibernético do Banco Cédula, com o intuito de prevenir e reduzir os riscos relacionados à segurança da informação das operações praticadas pelo banco, assim como garantir a integridade dos dados financeiros e pessoais de seus clientes e colaboradores sempre respeitando o sigilo dos dados e informações, bem como para a proteção do funcionamento adequado dos sistemas institucionais em conformidade com as atividades praticadas pela instituição.

Além das informações propriamente ditas, esta Política também se aplica a todo e qualquer meio utilizado em uma das fases do ciclo de vida das informações.

As diretrizes têm por principais objetivos:

- I. Estar em conformidade com as normas definidas pela legislação e regulamentos vigentes que dispõe sobre a política de segurança cibernética, definindo padrões de segurança em tecnologia da informação que visem garantir a continuidade operacional do negócio;
- II. Orientar as ações de comportamento e segurança, minimizando riscos contra a integridade, sigilo e disponibilidade da informação e de seus elementos constituintes;
- III. Comunicar tempestivamente ao Banco Central do Brasil sobre ocorrências de incidentes e interrupções dos serviços relevantes, que configurem situação que possa impactar as atividades do Banco Cédula, bem como das providências para o retorno das atividades;
- IV. Definir procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis, ou que sejam relevantes para a condução das atividades operacionais da instituição;
- V. Monitorar serviços contratados;
- VI. Conscientizar os colaboradores a protegerem diligentemente os ativos de informação;
- VII. Estabelecer diretrizes que possam responder às mudanças dos negócios, da legislação, das normas regulatórias e da tecnologia;
- VIII. Servir de referência para auditorias, verificações de conformidade e determinação de responsabilidades.

2. Abrangência

Esta Política tem como público-alvo todos os diretores e colaboradores do Banco Cédula, bem como prestadores de serviços que realizem atividades em seu nome.

3. Vigência e Atualizações

As diretrizes contidas nesta Política entram em vigor na data de sua publicação e permanecem vigentes por prazo indeterminado, devendo ser mantidas atualizadas e revisadas anualmente, de acordo com a alteração de legislação aplicável, ou ainda, se houver alteração no modelo de negócios, devendo, em qualquer caso, ser previamente validada pelo Departamento de Compliance.



CNPJ/MF: 33.132.044/0001-24

4. Diretrizes

As diretrizes e regras estabelecidas abaixo devem ser interpretadas como determinações obrigatórias:

- Toda e qualquer pessoa que possui acesso às informações da instituição devem estar cientes e concordantes com esta Política antes de ser concedido os acessos. As violações desta Política podem levar a revogação dos privilégios de acesso, incluindo responsabilização nas esferas cíveis, administrativas e penais, conforme o caso;
- Interpretações (questões ou exceções) desta Política são de ÚNICA e exclusiva responsabilidade da área de Gestão de Riscos e passíveis de aprovação pela Diretoria, conforme o caso;
- Notificações de incidentes de segurança assim que constatados devem ser efetuadas imediatamente para a Diretoria Responsável pela Gestão de Risco Operacional;
- A manutenção da segurança das informações, dos sistemas informatizados e ativos de informação é de responsabilidade de cada colaborador com acesso autorizado às mesmas.

Esta política é regulamentada, onde cabível e necessário, pela legislação e regulamentos vigentes, bem como por procedimentos definidos pela Diretoria e/ou Conselho de Administração do Banco Cédula.

5. Governança de Segurança da Informação

As informações tratadas, conforme determinado no artigo 5º, X da LGPD, pelo Banco Cédula são consideradas patrimônio ativo e confidencial. No caso de exceção, informações cuja divulgação seja obrigatória ao mercado e clientes por exigência de órgãos reguladores deve ser cuidadosamente avaliada e passar por autorização da Diretoria com o consentimento do proprietário da informação. Tal autorização deve ser respeitada durante todo o ciclo de vida desta informação.

A infraestrutura de tecnologia da informação do Banco Cédula mantém mecanismos e repositórios para manutenção de trilhas de auditoria, logs e demais notificações de incidentes, além de softwares de proteção contra malware/antivírus em toda a rede. A diretoria de Gestão de Riscos é acionada a qualquer tentativa de violação que seja informada ou detectada, tomando as medidas cabíveis para prover uma defesa ativa e corretiva contra os ataques empreendidos ou incidentes que os envolvam.

A tecnologia da informação utilizada nos negócios do Banco Cédula deve possuir documentação que permita a continuidade e o controle dela, independentemente de ter sido desenvolvida internamente ou por terceiros, garantindo-se sempre 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.

Os responsáveis pela segurança da informação e ativos tecnológicos devem desenvolver e usar mecanismos que protejam e garantam a continuidade dos processos. A necessidade e o tipo de contingência serão determinados com base na importância para o negócio e o tempo de indisponibilidade aceitável para este recurso, sem afetar a continuidade dos negócios do Banco Cédula.

Entende-se como interrupção relevante aquela que superar o prazo de 3h sem que haja o



CNPJ/MF: 33.132.044/0001-24

reestabelecimento das atividades, ainda que em contingência.

O acesso aos recursos da informação deve ser controlado e liberado através de autorização formal solicitada pelo gestor da área que necessite dos recursos. Essa autorização formal é solicitada via e-mail para a área competente.

Todos os recursos da informação, sejam eles tecnológicos ou não, devem ser utilizados exclusivamente para o desenvolvimento de atividades profissionais referentes aos negócios do Banco Cédula.

A identificação do usuário deve permitir o seu claro reconhecimento e, no caso de credenciais de acesso a sistemas e ativos tecnológicos, deve ser único, pessoal e intransferível. Eventuais danos e incidentes causados pelo uso indevido de credenciais de acesso e identificação, mesmo por parte de terceiros, serão de inteira responsabilidade do dono da credencial, incluído crachás, certificados digitais, token e senhas.

Todos os recursos da informação devem ser devidamente inventariados conforme suas características, de tal maneira que possam ser identificados de forma individual e única. Este processo de inventário deverá ser atualizado periodicamente, a fim de garantir sua consistência.

Os recursos da informação homologados e autorizados para uso deverão ser de propriedade do Banco Cédula ou ter seus direitos de uso cedidos, arrendados ou alugados. Tais recursos devem, obrigatoriamente, estar em conformidade com a legislação brasileira vigente.

Não deve ser utilizado dentro das dependências do Banco Cédula nenhum recurso da informação de procedência pessoal, mesmo que para fins profissionais, à exceção de recursos previamente autorizados pela área de Gestão de Riscos e/ou pela Diretoria.

Toda informação que deixe de ter utilidade para o Banco Cédula deverá ser destruída, sem possibilidade de recuperação, respeitados os prazos legais de manutenção da informação definidos pela legislação em vigor.

A segurança das informações contidas em qualquer equipamento portátil utilizado deverá seguir, no mínimo, os mesmos cuidados dos equipamentos equivalentes em uso internamente na empresa. A segurança física do equipamento portátil será de responsabilidade do seu usuário, e este deve respeitar as orientações fornecidas por quem disponibilizar tal recurso.

Ao final do expediente e sempre que necessário ausentar-se da mesa de trabalho todos os colaboradores devem ter o cuidado de bloquear/desligar seus computadores e guardar documentos confidenciais em local fora da visão e alcance de pessoas não autorizadas. Deve-se também evitar conversas sobre informações sigilosas em ambientes onde a confidencialidade da informação não poderá ser garantida.

O acesso como administrador aos sistemas em nuvem de ambientes produtivos ou que possuam dados sensíveis de infraestruturas, plataformas e softwares/funções, como serviço, devem ser restritos aos administradores da nuvem. Qualquer tipo de exceção deverá ser previamente autorizado pela Diretoria e pela área de Gestão de Riscos.

Caso algum colaborador perceba o descumprimento de alguma das diretrizes desta Política, deverá comunicar seu superior direto ou ao Departamento de Compliance.

O não cumprimento das diretrizes desta Política, seja intencional ou não, sujeita o colaborador a sanções administrativas, cíveis e criminais na forma da lei.



6. Classificação das Informações

A informação será determinada em 4 (quatro) fases:

6.1) Inventário dos Ativos

Identificar quais informações estão sob a posse do Banco Cédula e quem são os responsáveis por elas. Essas informações podem estar em formato de documentos eletrônicos, sistemas de informação, banco de dados, documentos em papel, sistemas de armazenamento em nuvem, locais ou em dispositivos, gravações de conversas telefônicas ou por mensageria, entre outros.

6.2) Classificação da Informação

As informações devem ser classificadas pelos seus responsáveis e usuários, utilizando as seguintes regras:

- I. **Confidencial:** deve-se pedir autorização para o dono da informação antes de copiar ou compartilhar com alguém (mesmo que seja interno). Exemplos: Novos produtos em fase de desenvolvimento, dados de clientes, arquiteturas e estratégias corporativas.
- II. **Interna:** a informação deve ser utilizada somente pelos colaboradores do Banco Cédula. Deverá ser pedido autorização da mesma forma que o confidencial, caso precise enviar para terceiros ou parceiros. Exemplos: Normas, Processos e Políticas, relatórios.
- III. **Pública:** pode ser compartilhado com todos. Exemplos: políticas públicas, explicação de produtos, informações públicas, legislação, documentos públicos (Escrituras, atos sociais e demais documentos públicos).

6.3) Rotular a Informação

Uma vez que a informação tenha sido inventariada e classificada, elas devem ser rotuladas.

O rótulo poderá ser feito em algumas ocasiões colocados automaticamente por sistemas que automatizam o processo (exemplo no envio de e-mails e serviços de armazenamento na nuvem do Banco Cédula), mas é altamente orientado que o próprio colaborador e dono da informação faça isso.

Documentos eletrônicos e mídias removíveis gerados pelos colaboradores do Banco Cédula devem possuir a classificação da informação, conforme orientado nesta norma e feita pelo próprio colaborador.

Sistemas, banco de dados, componentes tecnológicos, e serviços em nuvem devem ser classificados pela área de TI.

6.4) Tratamento da Informação

É de responsabilidade do utente da informação exigir e verificar se as informações classificadas estão em conformidade com as diretrizes estabelecidas na presente política, caso contrário deverá reportar para a área de Gestão de Riscos e/ou Departamento de Compliance sua desconformidade para a correta qualificação, devendo, até que seja reclassificada a informação, tratá-la como Interna sob pena de responsabilidade.

7. Instalação de Software e Hardware

Toda instalação de software e hardware deve ser feita pela área de Tecnologia da Informação (TI), sendo que todos os softwares e hardwares devem ser homologados e licenciados.

Qualquer software que, por necessidade do serviço, precisar ser instalado, deverá ser homologado pela



CNPJ/MF: 33.132.044/0001-24

área de TI e só assim serem disponibilizados para a área requerente.

É terminantemente proibido o uso de softwares ilegais(sem licenciamento)pelo Banco Cedula.

Toda aquisição e manutenção de sistema deve zelar pela observância dos princípios de controle sobre informações processadas e armazenadas,incluindo a adequada segregação de perfis de acesso e ao controle de vazamento de informações.

Após a aquisição e implantação do novo hardware e software, será atualizado o bem no Inventário de TI e nos controles de licenças de software.

A habilitação de usuários para uso dos softwares de rede ou em nuvem, será realizado mediante senha de acesso.

A área de Segurança da Informação poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso.

7.1. Sistemas Operacionais

Os sistemas operacionais,ferramentas e componentes físicos são implantados e configurados pela TI.

Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados, mediante a validação de senha. A autorização dos acessos aos sistemas é definida por meio das regras e normas de Segregação de Acessos.

É desabilitado aos usuários implantar novos sistemas, ferramentas e componentes básicos ou alterar quaisquer configurações sem a permissão formalizada e efetuada pela área de TI. Ainda assim, não são permitidos:

- Executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços;
- Executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa;
- Enviar informações confidenciais (autorizadas) para e-mails externos sem proteção.

No mínimo, o arquivo deve contar com a proteção de uma senha“robusta”, controle de acesso lógico.

7.2. Serviços em nuvem

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada, no prazo de 10 dias da contratação, ao Banco Central do Brasil contendo no mínimo as seguintes informações:

I - a denominação da empresa a ser contratada;

II - os serviços relevantes a serem contratados; e

III - a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, no caso de contratação no exterior.



8. Controle de Acesso Lógico

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividades envolvidas obesta identificação.O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal e deve respeitar as seguintes premissas:

- I. Utilizar senha de qualidade, com pelo menos oito caracteres alfanuméricos e caracteres especiais (símbolos). Orienta-se a não utilizar como senha informações pessoais fáceis de serem obtidas, tais como, nome, número de telefone ou data de nascimento;
- II. Não incluir senhas em processos automáticos de acesso ao sistema, como por exemplo, armazenadas em macros ou teclas de função.

Todas as senhas geradas pela TI, seja ela de um novo acesso ou quando bloqueada, deve ser alterada pelo colaborador/usuário no primeiro acesso, cadastrando uma nova senha conforme os padrões estabelecidos pela área de TI.

Além disso, os usuários devem alterar a senha de rede a cada 90 (noventa) dias, sendo que o sistema irá enviar notificações para a alteração da mesma 10 (dez) dias antes da expiração.

9. Estação de Trabalho

A estação de trabalho disponibilizada para o usuário tem por objetivo o desempenho das atividades profissionais do colaborador/usuário no Banco Cédula.

As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.

A integridade física e o perfeito funcionamento da estação de trabalho, são de responsabilidade do colaborador/usuário, seguindo as regras e orientações fornecidas pela Segurança da Informação.

São responsabilidades do usuário/colaborador:

- Encerrar a estação de trabalho no final do expediente, desligando o equipamento;
- Quando ausentar-se da mesa, o usuário/colaborador deverá bloquear a estação de trabalho e ativá-la com sua senha de acesso (Obs. Esta ação aplica-se a todos os usuários/colaboradores com estações de trabalho, incluindo equipamentos portáteis);
- Caso o usuário/colaborador não realize o bloqueio da estação de trabalho, ela será bloqueada automaticamente após um período de inatividade;
- Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo ao Banco Cédula, só devem ser utilizadas em equipamentos com controles adequados.

9. Mídias Removíveis

O uso de mídias removíveis no Banco Cédula não é estimulado, devendo ser tratado como exceção à regra.



CNPJ/MF: 33.132.044/0001-24

As mídias removíveis são o principal ponto de vulnerabilidade de segurança, podendo ser usadas para a fuga de informações corporativas confidenciais, sendo, portanto, bloqueadas como regra em todos os equipamentos da instituição.

Para liberação de mídias removíveis dos desktops e notebooks é necessário justificar o uso e aprovação pela área de Gestão de Riscos.

10. Acesso Remoto

O Banco Cédula permite o acesso remoto pelos colaboradores em posições chave, conforme determinação da Diretoria de acordo com a seguinte regra: o colaborador deve ser devidamente cadastrado no grupo de segurança do firewall, ter o certificado instalado em seu computador e conectar-se através de uma TEAMVIEWEAR.

Ademais, os Colaboradores autorizados são instruídos a:

- I. Manter softwares de proteção contra malware/antivírus nos dispositivos remotos;
- II. Relatar ao Compliance e área de Gestão de Riscos qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações do Banco Cédula durante o trabalho remoto;
- III. Não armazenar informações confidenciais ou sensíveis em dispositivos pessoais.

11. Equipamentos Particulares

Qualquer dispositivo computacional particular/terceiro para ser usado na rede corporativa, precisa ser avaliado e aprovado pela Área de Gestão de Riscos.

O Banco Cédula possui para comodidade dos visitantes, fornecedores e colaboradores, redes de acesso à internet distintas das redes da corporativa da empresa. Todas as redes são monitoradas e controladas para garantir o bom uso da infraestrutura.

12. Internet

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

O acesso às páginas e websites é de responsabilidade de cada usuário, ficando vedado o acesso a sites com conteúdo impróprio e páginas de relacionamento.

Os acessos à internet são monitorados através de identificação e autenticação do usuário.

13. E-mail

As regras na utilização do e-mail corporativo são:

- É vedado o uso de sistemas e-mail externos, não pertencentes ao Banco Cédula;
- O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através sistema oficial da empresa;
- É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a



CNPJ/MF: 33.132.044/0001-24

imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro;

- Evitar utilizar o e-mail da empresa para assuntos pessoais;
- Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria;
- Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela Segurança da Informação;
- Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, entre outros.

14. Monitoramento

Todos os colaboradores do Banco Cédula possuem o monitoramento dos seguintes canais:

- Ramais telefônicos;
- E-mails;
- Acesso à internet.

É efetuado a verificação do funcionamento dos monitoramentos feitos por amostragem mensalmente.

15. Segregação e Gestão de Acessos

A segregação de funções do Banco Cédula é criada usando os departamentos atrelados as funções executadas, facilitando assim a análise de conflitos de interesse e qualquer possível falha de concessão acesso.

A segregação de acessos lógica e física irá aplicar as análises feitas pela segregação de funções nos sistemas e ambientes físicos e virtuais do Banco Cédula.

As análises feitas pela segregação de funções consideram o máximo de acesso que um colaborador pode ter, porém a segregação de acessos poderá ter acessos mais restritos, afim de proteger o processo de erros comuns que podem ser causados por colaboradores que não possuem conhecimentos plenos dos processos.

16. Gestão de Acesso

16.1. Credenciamento

O credenciamento dos novos colaboradores deverá ser feito pelos administradores dos sistemas obedecendo as regras estabelecidas nos documentos vigentes de segregação de acesso aprovados



pela Diretoria.

16.2. Descredenciamento

O descredenciamento dos colaboradores ocorre no processo de desligamento ou término de contrato, não se importando o motivo da ocorrência. Todos acessos devem ser removidos pelo menos até ao final do dia.

16.3. Novos Acessos ou Novos Sistemas

A entrada de novos sistemas ou a necessidade de alterações dos acessos por mudanças sistemáticas ou ambientais podem ocorrer sem que tenha tempo hábil para uma análise formal da Diretoria. Nesses casos, a equipe de TI terá autonomia para decidir as melhores estratégias de acessos até que seja revisado e aprovado formalmente pela Diretoria.

17. Revisão de Acessos

A equipe de TI deverá pelo menos a cada 6 (seis) meses executar revisões completas sobre os acessos concedidos aos sistemas e ambientes do Banco Cédula.

Caso na revisão se identificado conflito nos acessos concedidos, e por questões internas a Diretoria entende que deverá manter tais acessos, caberá a Diretoria a aprovação destes acessos conflituosos.

18. Backup

A cópia de segurança (também conhecido como “backup”) deve possuir uma rotina de armazenamento que obedeça às orientações e estratégias descritas neste documento de tempo de retenção, confidencialidade e integridade da informação.

Os backups são realizados das 06:00h às 20:00h, a cada 1 (uma) hora, todos os dias. O período de retenção é de 7 (sete) dias semanais. As cópias de segurança são realizadas por empresa terceirizada especializada em serviços de *Cloud Computing*.

Com objetivo de manter a integridade da informação, o Banco Cédula além de realizar as rotinas de backup em todos os sistemas e softwares hospedados, também realiza o backup, cópia de segurança da máquina virtual garantindo a segurança das informações de processamento.

O processo de restauração das cópias de segurança também devem atuar em tempo hábil que possa atender a necessidade do negócio relacionado a incidentes e desastres.

Para garantir o restabelecimento dos serviços em caso de necessidade, serão realizados testes, a cada 6 (seis) meses, de restauração de cópias de segurança. Estes testes servem para familiarizar a equipe de TI com os processos de restauração, bem como afiançam a integridade dos dados dos backups.

19. Resposta a Incidentes

Um Plano de Ação e Resposta a Incidentes (PARI) deve incluir procedimentos para detectar, responder e para limitar os efeitos de um incidente de segurança.

OTI deve analisar constantemente possíveis falhas ou incidentes de Segurança que possam ocorrer no Banco Cédula, assim como também em seus parceiros/fornecedores críticos e criar possíveis planos de



CNPJ/MF: 33.132.044/0001-24

resposta para esses incidentes.

Caso seja constatado algum incidente relevante o mesmo deverá ser devidamente registrado pela TI com a análise da causa e o impacto na segurança da instituição, com o devido controle dos efeitos deste(s) incidente para as atividades institucionais através de relatório que deverá ser encaminhado ao departamento de Compliance e para a Área de Gestão de Riscos da Instituição para as providências necessárias e arquivo.

São considerados incidentes relevantes todo e qualquer incidente que possa, ainda que indiretamente, colocar em risco a integridade dos sistemas, da reputação da instituição ou de quaisquer de seus colaboradores ou vazamento de dados e informações internas ou sigilosas de quaisquer clientes ou da instituição, abrangendo, inclusive, informações recebidas de empresas prestadoras de serviços a terceiros.

Anualmente deverá ser elaborado relatório sobre a implementação do plano de ação e de resposta a incidentes pelo diretor responsável pela política de segurança cibernética e execução do plano de ação e resposta a incidentes a ser apresentado ao Conselho de Administração do Banco Cédula até o dia 31 de março do ano seguinte ao da data-base, qual seja, 31 de dezembro do ano de execução, contendo, no mínimo:

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

II - o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes em conformidade com as diretrizes da política de segurança cibernética;

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

IV - os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

20. Continuidade de Negócios

O Plano de Continuidade de Negócios contempla os principais sistemas e serviços da companhia deverá ser implantado e testado semestralmente, contemplando cenários de incidentes, a fim de reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

O plano de continuidade de negócios deverá ser aplicado dentro do menor prazo possível ao total reestabelecimento das atividades normais do Banco Cédula devendo os referidos testes de integridade ficarem arquivados à disposição do Banco Central pelo prazo legalmente definido.

21. Manutenção de Arquivos

O Banco Cédula manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Conformidade (Compliance) desta política, pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.



CNPJ/MF: 33.132.044/0001-24

22. Exceções

Situações que não se encaixem ou estejam em desacordo com esta política, deverão ser submetidas ao Compliance, que analisará as circunstâncias e fundamentos, e deliberará em conjunto com a Diretoria a aprovação para tal exceção.

Anualmente será revisada a presente Política

Área responsável pela Confecção	Diretoria de Riscos e Compliance; Diretoria de TI
Área responsável pela Aprovação	Conselho de Administração
Vigência	A contar de 20/12/2025