	POLÍTICA	**CÓDIGO: PG|09.00|03** **EDIÇÃO: 27/07/2023** **Nº de PÁGINAS: 28** **VERSÃO: 02** **ND: 01**

PG | Política de Segurança da Informação e Cibernética

Órgão elaborador: Tecnologia	**Órgão Validador: Diretor**

SUMÁRIO

1. OBJETIVO

Esta política tem com o objetivo estabelecer as “Diretrizes” e “Princípios” atribuições e responsabilidade, bem como as normas a serem estabelecidas com o intuito de assegurar os mais elevados padrões de segurança, controle e gestão de riscos e de governança no tratamento de informações armazenadas, processadas e transmitidas nos ambientes físico e virtual provendo orientação e apoio a Sociedade de acordo com os requisitos do negócio e com as leis e regulamentações relevantes, bem como a definição dos requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Essa política tem como base o porte, o perfil de risco e o modelo de negócio, assim como a legislação, as diretrizes e as melhores práticas aplicáveis, para atender, no âmbito do gerenciamento de risco operacional da Sociedade, aos 6 (seis) objetivos principais delineados pela regulamentação:

1. Acesso, de auditoria e de testes;
2. Contratação de serviço relevante;
3. Planos de contingenciamento e de extinção do contrato;
4. Localização de processamento e de armazenamento de dados;
5. Segurança física e a proteção de dados, de sistema e de sigilo bancário; e
6. Segurança cibernética
7. Disponibilidade, a integridade, a confiabilidade, a autenticidade da informação e a proteção de dados pessoais;
8. Notificação de incidente relevante.

2. DOCUMENTOS COMPLEMENTARES

Código de Conduta Ética

3. DOCUMENTOS DE REFERÊNCIA

Lei nº 13.709|18: Lei Geral de Proteção de Dados, que regula o tratamento de Dados Pessoais no Brasil, em meios físicos ou digitais_LGPD.

Lei nº 12.527|11: Lei de Acesso à Informação _LAI

Resolução CMN nº 4.968|21: Dispõe sobre a implantação e implementação de sistema de controles internos.

Resolução CMN nº 4.595|17: Dispõe sobre a política de conformidade das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Resolução CMN nº 4.557|17: Gestão integradas de Riscos.

Resolução CMN nº 4.893|21: Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Circular BCB nº 3.909|18: Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

4. DEFINIÇÕES, CONCEITOS E SIGLAS

Anexo	tabelas, Formulários, Dados, imagens ou figuras gráficas incorporadas às últimas páginas de uma Instrução Normativa, para ilustrar ou facilitar o entendimento e aplicação do seu conteúdo.
Ativos	são todos os elementos que detém algum tipo de valor para a Sociedade. Os ativos podem ser informações, hardwares (equipamentos), softwares (sistemas) e Funcionários / Colaboradores.
Ativos de informação	qualquer elemento que tenha capacidade de coletar, desenvolver, receber, transmitir, manusear, armazenar, trafegar ou descartar informações.
Ativos de *Software*	aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.
Ativos Físicos (*Hardware*)	equipamentos computacionais (computadores, processadores, monitores, notebooks etc.), equipamentos de comunicação (roteadores, PABX, smartphones, tablets etc.), mobília, acomodações.
Autoridade Nacional de Proteção de Dados (“ANPD”)	órgão da administração pública responsável, dentre outras competências, por cuidar, implementar e fiscalizar o cumprimento da LGPD.
BACEN	Banco Central do Brasil.
Certificados de chave pública	também conhecidos como certificados digitais ou certificados de identidade, são documentos eletrônicos que usam uma assinatura digital para vincular uma chave pública a uma identidade, informações como o nome de uma pessoa ou organização, seu endereço etc. podem ser usados para verificar se uma chave pública pertence a um indivíduo.
Ciclo de vida da informação	conjunto de fases composto por planejamento ou pré produção, produção, divulgação, transporte, armazenamento e descarte de informação e documento.
Código malicioso	termo genérico que se refere a todos os tipos de programa especificamente desenvolvidos para executar ações danosas em recursos de Tecnologia da Informação, tais como Vírus, Cavalo de Tróia*, Spyware*, *Worms*, entre outros.
Colaborador	Corresponde a qualquer colaborador(a) em regime de trabalho CLT, pró-labore, estágio ou outro regime juridicamente aceito, vinculado a Sociedade ou a sociedade afiliada, controladora ou

	controlada da Sociedade, que venha a ter acesso no exercício de suas funções a informações detidas e/ou sob o seu controle.
Criptografia	conjunto de técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, tornando impraticável a leitura por pessoa não autorizada.
Custodiante	pessoa, setor ou área da Sociedade que mantém informação sob sua guarda. Dados pessoais: informações relacionadas diretamente a uma pessoa física identificada (ex.: número de telefone, e-mail, CPF, data de nascimento, identificadores eletrônicos), ou que podem levar à identificação de uma pessoa (ex.: GPS, redes WiFi, IDs de utilização de aplicações).
Diretrizes	Conjunto de padrões para gestão, estrutura organizacional, processos, procedimentos e recursos necessários à Gestão.
Diretoria	órgão da administração, formado pelos diretores estatutários da Sociedade. Disponibilidade (da informação): prevenção contra interrupções na operação de sistemas e no acesso à informação quando houver necessidade, de forma contínua, segura e eficiente.
Encarregado (pela proteção de dados pessoais)	pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares de dados e a ANPD.
Gerenciamento de Risco	processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável. Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação, protegendo-a de diversos tipos de ameaças, para garantir a continuidade de negócios, minimizar perdas e danos e maximizar o retorno dos investimentos e as oportunidades de negócio.
Incidente de segurança	evento adverso, confirmado ou sob suspeita, motivado por violação ou falha de um controle ou procedimento de segurança, seja de forma intencional ou não, com probabilidade de colocar em risco a segurança da informação.
Incidente cibernético	ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança cibernética.
Informação	Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento contidos em qualquer meio, suporte ou formato.

Informação sigilosa	informação submetida à restrição de acesso público por estar abrangida por hipótese de sigilo legal.
Princípios	preceitos elementares ou requisitos que a Sociedade deve observar na realização de suas atividades, buscando uma conduta exigida nos relacionamentos, operações e serviços, em seu ambiente interno ou externo.
Responsabilidade	consiste na obrigação de responder corporativa ou localmente por determinadas atribuições.
Risco cibernético	exposição de danos e perdas resultantes da ocorrência de incidentes cibernéticos.
Segurança da informação	ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade, e a autenticidade das informações.
Segurança cibernética	ações voltadas para preservar a disponibilidade, a integridade, a confidencialidade, e a autenticidade das informações.
Terceiros	entende-se tanto a entidade, quanto seu representante legal e/ou preposto que prestem ou estejam prestando serviços para a Instituição, como os prestadores de serviço em si, parceiros, franquias, fornecedores, auditores ou qualquer outro que se enquadre como prestador terceirizado.
Tratamento	toda operação realizada com dados, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão, ou extração.
Trilha de Auditoria	trilha de Auditoria ou log de Auditoria trata-se de um registro de todas as ações, eventos ou atividades que um usuário ou sistema realizou com seus dados. É usada para assegurar o fluxo preciso das transações desse sistema, funcionando como complexo e detalhado rastreamento. Dessa maneira podem estar relacionados à criação, modificação, exclusão de registros ou mesmo sequência de ações automatizadas do sistema.
Vulnerabilidade	conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema e que podem ser evitados por uma ação interna de segurança de informação.

5. ABRANGÊNCIA

Este documento é aplicável a todos os Colaboradores, parceiros, fornecedores e prestadores de serviços, incluindo os colaboradores de entidades externas ou outras entidades e/ou pessoas que atuem, direta ou indiretamente, em nome ou benefício da Sociedade, e que tenham acesso ou façam algum uso de suas informações, bem como observar em todo o conjunto de normas e procedimentos que formam a matéria, para mantermos a elevada confiabilidade e credibilidade de nosso ecossistema e honrarmos nosso compromisso para a garantia da confidencialidade, integridade e disponibilidade da informação.

6. DETALHAMENTO

6.1. Princípios

Os princípios são os pilares para as ações ou condutas de Segurança da Informação que atuam como um guia para a sua implementação e gestão. Dessa forma, considerando os princípios da confidencialidade, integridade, disponibilidade, autenticidade e não repúdio, algumas medidas técnicas e administrativas, conforme descritas nesta Política, são essenciais para garantir a proteção das informações da Sociedade pautar-se nos seguintes princípios:

Alinhamento estratégico	deve haver alinhamento entre políticas, normas e diretrizes de Segurança da Informação e os objetivos de negócio e o planejamento estratégico.
Autenticidade	propriedade pela qual se assegura que a informação foi produzida ou expedida, modificada ou destruída por uma pessoa natural, equipamento, sistema, órgão ou entidade.
Conformidade	aderência aos termos e responsabilidades contratuais, bem como aos controles de segurança da informação.
Confidencialidade	propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão ou entidade não autorizados nem credenciados.
Ética e Legalidade:	Atuação conforme a legislação e regulação vigentes, com padrões de ética e conduta. eficiência dos serviços.
Integridade	propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou incidental.
Irretratabilidade	princípio de segurança da informação por meio do qual é garantido o não repúdio às informações fornecidas.
Legalidade	Atuar sempre em conformidade com a legislação e regulação vigentes.
Melhoria contínua	Compromisso de aperfeiçoar os padrões de ética e conduta, aplicação de medidas corretivas, adequados níveis de segurança, qualidade dos produtos ofertados e

Transparência	reporte adequado das condições acordadas com a devida aplicação, bem como reflexos nas demonstrações contábeis.
Promover um ambiente positivo de segurança	a Segurança da Informação é construída sobre o comportamento humano. Este comportamento consiste no engajamento das equipes em desempenhar suas atividades de acordo com os parâmetros de segurança estipulados nesta Política, por meio de medidas educativas e de conscientização.
Propriedade da informação	toda informação produzida ou armazenada na Sociedade é de sua propriedade e não dos Colaboradores que nela trabalham, exceto nos casos em que a Sociedade atuar como Custodiante da informação de outra organização, quando a informação poderá pertencer a um terceiro.

6.2. Diretrizes

1. Preservar a confidencialidade, disponibilidade, integridade, sigilo e autenticidade das suas informações;
2. Orientar quanto ao uso adequado de seus Ativos e proteger as atividades finalísticas e a gestão**;**
3. Estabelecer medidas técnicas e administrativas capazes de proteger as informações, inclusivedados pessoais, contra acessos não autorizados e de situações acidentais ou ilícitas envolvendo a destruição, perda, alteração, comunicação ou vazamento de informação; e
4. Nortear a definição de procedimentos específicos de controles e processos para a gestão dos riscos de segurança da informação.
5. Os níveis gerencias devem zelar pelo cumprimento dessa política no âmbito de sua competência, dedicando especial atenção aos aspectos de segurança da informação e cibernética.

6.3. Dados coletados

Essa política destina-se a todas as informações coletadas, criadas, recebidas, armazenadas, processadas, transmitidas ou impressas, com o auxílio de qualquer sistema, meio de transmissão ou de armazenamento, por colaboradores, parceiros, fornecedores e prestadores de serviços, devendo estar disponível a todo tempo a todos, aos quais caberão ler atentamente e aceitar todo o seu conteúdo antes de obter acesso a qualquer Ativo ou informação da Sociedade.

É indispensável assegurar que todos, independentemente do seu nível hierárquico, função e/ou vínculo contratual, entidades externas ou outros contratados pela Sociedade tenha conhecimento desta política e acesso adequado à informação necessária para o desempenho das suas funções, sendo exigido destes o respeito pelos controles de segurança implementados e o cumprimento dos aspectos de integridade, confidencialidade e disponibilidade da informação, sendo estes, responsabilidade de todos.

6.4. Propriedade das informações

É de propriedade da Sociedade toda a informação gerada ou tramitada por meio dos seus recursos.

Toda informação de propriedade ou custodiada pela Sociedade:

1. Somente deve ser utilizada pelos colaboradores ou terceiros contratados para fins profissionais ou, em outros casos, com autorização formal, emanada por instância competente para fazê-lo;
2. Deve ser classificada segundo critérios definidos.
3. Deve ser protegida contra a modificação, destruição ou divulgação não autorizada, e principalmente quanto ao acesso de pessoas não autorizadas ou que não tenham direito ao seu conhecimento;
4. Deve ser armazenada, por tempo determinado pela empresa e/ou legislação vigente, e recuperada somente quando for necessária. Testes de *restore de "backup"* deve ser aplicado a cada encerramento do exercício.

6.5. Procedimentos

Os procedimentos, controles, mecanismos e ações adotadas pela Sociedade para alcançar os objetivos de Segurança da Informação e cibernética contemplam:

6.5.1. Gestão de Vulnerabilidades e Prevenção a Incidentes

Para o processo de gestão de vulnerabilidades, são estabelecidas diretrizes para a detecção, classificação e tratamento de vulnerabilidades de infraestrutura, aplicações e sistemas da Instituição.

Deve ser realizada análise Manual e Automatizada de vulnerabilidades de Segurança:

1. **Análise Automatizada:** Refere-se ao uso de ferramentas na esteira CI/CD. No momento da submissão (commit) de uma nova versão de software do ambiente de desenvolvimento para homologação, softwares de análise de segurança do tipo SAST e DAST deverão realizar inspeções com o objetivo de detectar vulnerabilidades. Na detecção, os times de Cyber Segurança e Desenvolvimento deverão ser notificados.
2. **Análise Manual:** Refere-se ao teste de Penetração aos sistemas alvo, utilizando a análise humana o teste de simular o comportamento de fraudadores ou especialistas em Cyber Segurança com o objetivo de identificar falhas de média e alta complexidade, assim como também falhas de segurança relacionadas ao negócio da Instituição.

As verificações de vulnerabilidades devem ser realizadas pelo menos semestralmente ou após qualquer alteração significativa no ambiente. Isso deve se aplicar a todos os ambientes que mantêm dados de produção.

Deverá ser realizada a avaliação dos ativos pertencentes à infraestrutura e aplicação, considerando a identificação dos componentes que podem expor a segurança.

Deverá ser apresentado um plano de trabalho para avaliar e reportar a situação atual da segurança do ambiente considerando:

1. Quebra dos controles de segurança estabelecidos para a proteção do ambiente.
2. Exploração das vulnerabilidades identificadas na infraestrutura e nas aplicações disponíveisnos endpoints alvos da análise. Conduzir prioritariamente testes do tipo Black Box.

Os testes de intrusão, sejam eles internos ou externos, devem ser realizados pelo menos uma vez por ano e/ou após qualquer atualização, modificação significativa da infraestrutura ou dos sistemas. Isso se aplica a todos os ambientes que mantêm dados de produção.

As falhas de segurança identificadas nos testes deverão ser tratadas com alta prioridade com

vistas a mitigar os riscos envolvidos, e os resultados obtidos através dos testes deverão ser devidamente registrados, sendo que as falhas que oferecerem "alto risco" deverão passar por um novo teste após a implementação das medidas de mitigação.

Além disso, são adotados controles para rastreamento e prevenção de vazamentos de informações baseadas no nível de classificação. Os controles adotados permitem a identificação de informações armazenadas em ativos, evidenciando informações sensíveis. As diretrizes contidas nesta Política permitem que diferentes ações sejam tomadas de acordo com o nível de sensibilidade e autorização que cada colaborador possui em relação a manipulação de informações, registrando eventos indevidos que servem como trilhas para o registro de incidentes que violem a segurança das informações manipuladas.

A Equipe de Segurança da Informação deverá acompanhar todo o processo a fim de obter informações necessárias para realização de uma gestão sobre as aplicações de correções de vulnerabilidade, essas informações alimentará o controle de Segurança da Informação para as vulnerabilidades do ambiente da Sociedade**.**

6.5.2. Gestão de *Patches*

O processo de gestão de *patches* é uma prática proativa destinada a prevenir, dentro da infraestrutura de tecnologia da informação, a exploração de vulnerabilidades que poderiam comprometer a confidencialidade, integridade ou disponibilidade das informações manipuladas por componentes dessa infraestrutura. Todos os Ativos de informação de propriedade ou mantidos pela Sociedade devem ter instalados os últimos *patches* estáveis, disponibilizados pelos respectivos fornecedores.

6.5.3. Senhas de Usuários

A política de senhas estabelece que elas sejam de uso confidencial, pessoal e intransferível, além de conter requisitos mínimos de segurança de acordo com o seu grau de criticidade.

Os sistemas, redes e aplicativos de informação devem ser protegidos pelo uso de senhas fortes para garantir que as informações não sejam divulgadas, modificadas, excluídas ou tornadas indisponíveis incorretamente.

A identidade de um usuário deve ser verificada, exigindo várias informações exclusivas do usuário antes da redefinição de uma senha. As credenciais do usuário (por exemplo, ID do usuário e senha) devem ser comunicadas separadamente.

A elaboração de senhas para acesso à rede ou aos sistemas deve ser realizada conforme abaixo:

1. Não utilizar a mesma senha para diversas finalidades;
2. Utilizar senha de no mínimo 8 caracteres, alfanuméricos, com caracteres especiais (@ # $ %) e variação de maiúsculo e minúsculo;
3. A senha não deve ser baseada em informações pessoais, como próprio nome, nome de familiares, data de nascimento e não deve ser constituída de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras;
4. Utilize um *software* gerenciador de senhas para gerar senhas fortes e armazená-las de forma segura;
5. Deverá ser utilizada a autenticação de dois fatores (2FA), exigindo que o usuário forneça dois meios de identificação antes de conseguir se autenticar.

Os critérios para elaboração, manutenção e gerenciamento dos acessos devem levar em consideração a criticidade das informações e as necessidades dos processos de negócio envolvidos.

6.5.4. Gestão de Acessos

Todas as informações, sistemas, redes e aplicativos devem ser protegidos através do uso de controles de acesso lógico para garantir que as informações não sejam divulgadas, modificadas, excluídas ou tornadas indisponíveis indevidamente.

Os acessos aos ativos de informação e aos recursos computacionais e de comunicação da Sociedade devem estar relacionados com os seus negócios, exclusivamente.

No ato da contratação, mudança de área ou desligamento de Funcionários / Colaboradores e Terceiros, deve-se existir processos que registrem, revisem e ajustem os acessos físicos e lógicosde acordo com as novas funções desempenhadas e que tenham acesso somente às informaçõese recursos que sejam necessários ao seu cargo ou função.

A informação deverá ser acessada de acordo com os controles de acesso existentes e deverá ser tratada com observância às finalidades para as quais foram criadas ou coletadas, respeitando-se, naquilo que for cabível, os princípios da necessidade e finalidade, sempre e exclusivamente para os fins corporativos.

A identificação de cada Funcionário / Colaborador para fins de acesso (usuário e senha), deverão ser de uso único, pessoal e intransferível, qualificando o respectivo como o responsável pelas ações realizadas com a sua identificação, exceto quando comprovada fraude ou subtração.

As regras de controle de acesso e de direitos de uso para os proprietários de informação devem contemplar cada usuário individual ou grupos de usuários.

Os sistemas de informação utilizados na Sociedade deverão ser acessados apenas por Funcionários / Colaboradores identificados. Cada usuário deve estar restrito a apenas uma conexão por sistema, em um dado instante.

Deve ser obrigatória a utilização de controle de acesso baseado em biometria nas instalações físicas da Instituição, a fim de impedir o acesso não autorizado, danos e interferências nos recursos de processamento de informações.

6.5.5. Concessão de Acesso

1. A licença para a utilização dos recursos de Tecnologia da Informação é uma concessão da Sociedade aos Funcionários / Colaboradores que necessitam deles para desempenhar suas funções. A utilização poderá ser monitorada em tempo real e a licença poderá ser suspensa a qualquer momento por decisão do Gestor da área do colaborador, da área de tecnologia ou da área de RH, de acordo com os exclusivos critérios destes, visando evitar perda de produtividade e riscos de segurança.
2. Acesso à consulta ou utilização dos recursos de Tecnologia da Informação é permitido após a identificação do usuário, somente por meio de suas próprias credenciais de acesso.
3. As credenciais de acesso aos recursos de Tecnologia da Informação são pessoais, intransferíveis e de responsabilidade exclusiva do colaborador.
4. Toda solicitação, alteração, bloqueio e desbloqueio de acesso aos recursos de Tecnologia da Informação ou aos sistemas deve ser documentada e solicitada através de sistema definido pela área de TI.

5. Gestor da área do Funcionário / Colaborador, deve informar à área de tecnologia todos os direitos de acesso que o usuário deve possuir.
6. Todos os direitos de acesso aos recursos de Tecnologia da Informação devem ter prazo de vigência definido.
7. É expressamente proibida qualquer tentativa de acesso não autorizado aos recursos de Tecnologia da Informação.

Procedimentos de controle de acesso físico devem ser implementados de forma a restringir o acesso às áreas protegidas e seguras. Os procedimentos de controle de acesso devem, quando necessário, contemplar, entre outros:

1. A utilização de dispositivos de identificação pessoal;
2. Monitoração de acessos;
3. Restrições de horários de acesso e permanência;
4. Controle de acesso de terceiros;
5. Movimentação de ativos;
6. O pessoal autorizado deve ter acesso físico somente aos ativos imprescindíveis para a realização dos seus trabalhos.

6.5.6. Concessão de Acesso Privilegiado

Devem ser identificados todos os Ativos ou grupos de Ativos da Instituição, classificando-os quanto ao nível de confidencialidade da informação, a fim possibilitar a criação, uso, monitoramento, e gestão de acessos privilegiados, os quais habilitam usuários autorizados a executar tarefas que usuários comuns não tem permissões para realizar.

1. Os usuários privilegiados deverão usar sua conta de Administrador exclusivamente vinculada ao indivíduo que está usando a conta. Essa conta deve ser distintamente diferente da conta de uso geral do usuário ("Não privilegiada");
2. Contas privilegiadas não devem ser associadas a nomes de computadores, nomes de departamentos, cargos ou qualquer outra informação semelhante que possa revelar a natureza privilegiada da conta;
3. Contas privilegiadas devem ser usadas apenas quando necessário e devem ser desconectadas imediatamente após o uso;
4. Um inventário de contas privilegiadas deve ser estabelecido, mantido, revisado e aprovado periodicamente pela área de tecnologia e segurança da informação;
5. Devem ser estabelecidos registros e monitoramentos auditáveis para emitir um alerta de múltiplas tentativas malsucedidas em efetuar login em uma conta administrativa.

6.5.7. Proteção Contra Código Malicioso

Devem ser implementados controles para prevenção e detecção de *softwares* maliciosos em todos os Ativos de tecnologia da Informação, com base nas diretrizes abaixo:

1. Os recursos de Tecnologia da Informação devem estar providos de sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, tais como programas antivírus, programas de análise de conteúdo de Correio Eletrônico e *firewall*;
2. Havendo correções ou atualizações para os sistemas de detecção e bloqueio de códigos maliciosos, as mesmas devem ser implementadas, a fim de se evitar que estes sistemas fiquem vulneráveis a códigos maliciosos ou a qualquer tentativa de acesso não

autorizado;

3. As atualizações e as correções para os sistemas de detecção e bloqueio na segurança do perímetro e nuvem devem ser homologadas em ambiente controlado antes de aplicadas ao ambiente de produção;
4. É obrigatório o uso de sistemas de detecção e bloqueio de códigos maliciosos em todos os recursos de Tecnologia da Informação;
5. Os sistemas de detecção e bloqueio de códigos maliciosos devem prover o monitoramento, em tempo de execução, dos arquivos e programas, quanto à contaminação por código malicioso;
6. Arquivos ou mídias que são utilizados nos equipamentos computacionais devem ser verificados automaticamente, quanto à contaminação por código malicioso, antes de sua utilização;
7. Os arquivos anexados às mensagens de Correio Eletrônico, logo após seu recebimento, devem ser verificados, quanto à contaminação por código malicioso, através do software antivírus homologado e instalado nas estações de trabalho dos colaboradores;
8. Os arquivos contaminados por código malicioso devem ser imediatamente descontaminados pelo software antivírus, isolados ou removidos do sistema. Em caso de persistência do problema, o equipamento deve ser isolado até que seja sanado o problema para não afetar o ambiente de produção;
9. Padrões e procedimentos para instalação, configuração, utilização e atualização de sistemas de detecção e bloqueio de códigos maliciosos devem ser estabelecidos pela área de tecnologia.

6.5.8. Segurança de Rede

Toda a comunicação entre as redes da Sociedade e a Internet ou qualquer outra rede pública devenecessariamente passar por um sistema de controle de acesso de conexões (Firewall), configurado com política restritiva, com monitoramento bidirecional dos fluxos de comunicação e com proteção contra-ataques, tais como negação de serviço, entre outros.

Toda comunicação entre computadores remotos e as redes, através da Internet ou outra rede pública, deve ser autenticada e criptografada, usando soluções tecnológicas autorizadas pela áreade Tecnologia da Informação.

6.5.9. Cópias de segurança *(backup)*

A realização de cópias de segurança (*backups*) deve obedecer aos procedimentos internos, com o objetivo de garantir a realização e monitoramento das cópias de segurança.

As diretrizes abaixo descrevem os métodos e requerimentos para a realização de backup de dados, as funções de armazenamento, manipulação e replicação durante o processo de backup.

Os administradores de armazenamento, servidor e banco de dados devem utilizar soluções e recursos de nível empresarial, que incluem métodos avançados para backup, arquivamento e restauração de dados;

1. Os backups devem ser concluídos regularmente;
2. Os registros das cópias de backup serão mantidos e incluirão o conteúdo e a localização atual;
3. Os procedimentos de restauração serão documentados pela equipe de TI;

4. Quando o serviço de backup é realizado por terceiros, o contrato de nível de serviço deve incluir proteções para controlar a confidencialidade, a integridade e a disponibilidade dos dados;
5. A equipe de TI deve testar as restaurações do backup semestralmente. O teste de backup deve ser limitado aos dados e sistemas críticos da Instituição;
6. A equipe de TI deve monitorar os processos de backup em busca de falhas nas rotinas e tomar as medidas necessárias para corrigir e documentar todos os problemas;
7. As cópias de segurança devem ser executadas nos sistemas de arquivos de produção;
8. Instantâneos (snapshots) dos servidores de produção, quando aplicável, devem ser usados para garantir a configuração dos servidores e a integridade dos dados;
9. A replicação de dados de produção deve ser sincronizada de maneira confiável (contingência);
10. Não deve haver manipulação de dados do armazenamento externo de mídia sem autorização prévia da Área de Segurança da Informação;
11. Se necessário, uma lista global de exceções deve ser mantida para excluir o backup de arquivos que não requerem proteção de backup.

6.5.9.1. Armazenamento

1. Os *backups* externos precisam ser identificados de forma clara, contendo o nome, data, hora e categoria (*Full* / Incremental);
2. Os backups devem ser armazenados em um local remoto fisicamente seguro, a uma distância suficiente para torná-los imunes a danos aos dados no ambiente primário;
3. Todos os logs de backup devem ser armazenados em um repositório dedicado; importante não separar os "*logs" de backup*.

6.5.10. Criptografia e gerenciamento de chaves

O uso efetivo e adequado de um sistema de criptografia deve ser estabelecido com o intuito de assegurar a confidencialidade, autenticidade e integridade das informações sensíveis. Todos os sistemas, controles, ferramentas, técnicas ou soluções de criptografia devem ser aprovados pela área de tecnologia. A área de Tecnologia da Informação deve executar revisões de criptografia e gerenciamento de chaves periodicamente, ou mediante alterações significativas de tecnologias. Os proprietários do sistema são responsáveis por estabelecer e manter uma descrição documentada da arquitetura criptográfica, incluindo:

1. Detalhes de algoritmos, protocolos e chaves, incluindo a força das chaves e a data de validade;
2. Descrição do uso da chave para cada chave criptográfica;
3. Inventário de qualquer HSM (*Hardware Security Modules*) e outros dispositivos criptográficos seguros usados para gerenciamento de chaves.

6.5.11. Utilização dos ativos de tecnologia da informação

Os Ativos de tecnologia da informação são recursos corporativos, de propriedade da Instituição, disponibilizados apenas para a execução das atividades funcionais dos Funcionários / Colaboradores.

6.5.11.1. Acesso e Utilização do Correio Eletrônico

1. O serviço de Correio Eletrônico corporativo é uma concessão da Sociedade, sendo assim, seu uso é permitido somente para as atividades profissionais de seus colaboradores, não sendo permitido enviar ou arquivar mensagens não relacionadas às atividades profissionais, que contenham:

2. ·Assuntos que provoquem assédio, perturbação a outras pessoas ou que prejudiquem aimagem da Instituição;
3. ·Temas difamatórios, discriminatórios, material obsceno, ilegal ou antiético;
4. ·Fotos, imagens, sons ou vídeos que não tenham relação com as atividades profissionais da organização;
5. As permissões de acesso a serviços de e-mail particulares, tais como webmail, podem ser estabelecidas, autorizadas e gerenciadas pela área de tecnologia, em função dos interesses da Instituição;
6. O acesso ao Correio Eletrônico corporativo se dá pelo conjunto “Identificação do Usuário e Senha”, que é pessoal e intransferível;
7. O endereço de e-mail disponibilizado ao usuário é de uso pessoal e intransferível e de responsabilidade dele. Portanto, é terminantemente proibido suprimir, modificar, ou substituir a identidade do remetente ou destinatário de uma mensagem do Correio Eletrônico;
8. A disponibilização do Correio Eletrônico pode ser suspensa a qualquer momento por decisão do Gestor da área do colaborador ou da área de Tecnologia da Informação;
9. As concessões e revogações de acesso ao serviço de Correio Eletrônico devem ser autorizadas pelo Gestor da área do usuário ou pela área de RH, por meio de uma solicitação de serviço à área de tecnologia;
10. Os anexos das mensagens de Correio Eletrônico poderão ser bloqueados quando ofereceremriscos à Segurança da Informação;
11. A abertura de mensagens de remetentes desconhecidos, deve ser avaliada, especialmente quando houver dúvidas quanto à natureza do seu conteúdo, como arquivos anexados não esperados ou hiperlinks para endereços externos não relacionados às atividades profissionais;
12. As mensagens encaminhadas para remetentes internos e externos não devem conter números de cartões e/ou outras informações pessoais, sem o devido tratamento de mascaramento dos números;
13. Todas as mensagens originárias de Colaboradores da Instituição deverão conter a assinatura do remetente em formato padronizado, além de um aviso legal, também padronizado, referenciando a confidencialidade da informação.

6.5.11.2. Uso da Internet

1. É permitido o acesso a sites que sejam fontes de informação necessária à execução das atividades profissionais na Instituição;
2. Não devem ser usados os recursos de “Salvar Senha” ou “Lembrar Senha”, disponíveis na maioria das aplicações, devendo ser desmarcada sempre que for apresentada esta opção. Senhas não devem ser incluídas em nenhum outro processo de autenticação automática disponível;
3. Quando estiver usando a Internet e verificar que o site acessado contém conteúdo impróprio, o usuário deve abandonar o site e abrir um incidente de Segurança da Informação;
4. Não é permitido o uso de aplicações ponto-a-ponto (*peer-to-peer*) para distribuição de arquivos, tais como aplicativos Torrent, Emule e correlatos;

5. Não é permitido o uso de jogos *on-line*.

6. Ressalvado os interesses da Sociedade, não é permitido:

a. Acesso a conteúdo impróprio, que são aqueles relativos à pornografia, racismo, violência, incitação ao ódio, invasão de computadores, jogos, entre outros;

b. Não é permitido o acesso à internet para fins de atividades ilícitas;

c. Uso de serviços de mensagem instantânea, que não seja a utilizada e chancelada pela área de Tecnologia da Informação;

d. A sondagem, investigação ou teste de vulnerabilidade em computadores, através da Internet ou de outra rede pública, exceto quando autorizada pela área de Tecnologia da Informação.

6.5.11.3. Segurança Física

1. As instalações da Instituição devem estar protegidas contra acesso não autorizado, sendo obrigatório o registro de entrada e o registro de saída de todos os diretores, empregados, prestadores de serviços terceirizados e visitantes. A autorização de acesso deve ser aprovada e liberada por empregado com alçada para essa ação.

2. Todos os prestadores de serviço enquanto presentes no ambiente da Sociedade devem estar devidamente identificados e acompanhados por um Funcionário / Colaborador.

3. A presença de uma pessoa não autorizada em área de acesso controlado caracteriza um Incidente de segurança que deve ser reportado à área de Segurança da Informação.

6.5.12. Gestão de mudanças

O processo de gestão da mudança tem como objetivo assegurar que as mudanças nos sistemas de TI sejam controladas e gerenciadas consistentemente a fim de manter a disponibilidade dos sistemas de produção, minimizar o risco de falhas do sistema, garantir aprovações apropriadas (via Comitê) e apoiar a Auditoria nas mudanças em produção, de acordo com os padrões estabelecidos nesta Política.

As atualizações de configuração no ambiente de produção devem ser realizadas, inicialmente, em ambiente de teste ou homologação e, todo software deve ser analisado criticamente, considerando os seguintes aspectos:

1. Análise crítica dos procedimentos de controle e integridade do software, garantindo que eles não foram comprometidos pelas mudanças efetuadas no ambiente de produção.

2. Revisão do planejamento e do orçamento anual de tecnologia, garantindo investimentos pararevisões e testes de softwares resultantes das modificações do ambiente de produção;

3. Revisão do Plano de Continuidade dos Negócios para contemplar mudanças necessárias resultantes das modificações do ambiente de produção.

6.5.13. Gestão de continuidade do negócio

A Sociedade deve implementar planos de continuidade dos negócios documentados, testados e revisados periodicamente, de forma que seus serviços essenciais sejam devidamente identificados, contemplando os mecanismos de Segurança da Informação estabelecidos nos ambientes de produção.

Estruturar o entendimento integral de todos os aspectos e fenômenos relacionados à continuidade do negócio, incluindo:

1. Identificação das ameaças potenciais e os respectivos impactos nas operações do negócio;
2. Definição da estratégia de recuperação a ser utilizada caso ocorra um incidente;
3. Gerenciamento de Crise para incidentes adversos que interrompam um processo crítico;
4. Planejamento da continuidade e da recuperação das operações e sistemas após uma interrupção;
5. Estabelecimento de procedimentos de retorno à normalidade, quando aplicável;
6. Incorporar a gestão da continuidade de negócio ao desenvolvimento de novos produtos e serviços críticos e ao processo de gerência de mudanças para produtos e serviços existentes;
7. Prover a continuidade das operações do negócio em um nível aceitável pré-definido;
8. Aumentar o poder de recuperação da organização contra o rompimento ou interrupção de sua habilidade de fornecer seus produtos e serviços;
9. Orientar ações de prevenção e mitigação dos riscos operacionais;
10. Prover a organização de uma metodologia para a elaboração de planos de continuidade de negócios que possibilite o restabelecimento da sua habilidade de fornecer seus produtos e serviços críticos;
11. Gerenciar o Programa de Continuidade de Negócios por meio de treinamentos, testes e análises que garantam o bom funcionamento dos Planos de Continuidade.
12. Fixar normas e padrões de continuidade, compondo assim, um programa completo e consistente para a organização, devendo ser aceito e seguido inclusive pelas empresas prestadoras de serviço.

Deve haver redundância dos Ativos de informação da empresa, para que estes atendam aos requisitos de disponibilidade.

6.5.14. Classificação da informação

Todas as informações custodiadas ou de propriedade da Sociedade devem ser classificadas em uma das seguintes categorias:

Pública: informações de caráter informativo, profissional ou que, em função da legislação vigente, são divulgadas a todo o público interno e externo, mediante a avaliação da Assessoria de Comunicação ou Unidade equivalente.

Interna: informações pertencentes ou custodiadas pela Sociedade, que podem ser acessadas por todos os colaboradores, mediante autorização do respectivo proprietário.

Confidencial: informações pertencentes ou custodiadas pela Sociedade e que, se reveladas, podem trazer impactos negativos aos negócios ou repercussões para a imagem dele, embaraços administrativos com colaboradores ou vantagens a terceiros e outras informações protegidas por legislação específica.

6.5.14.1. Recomendações para classificação:

1. Informação "pessoal" não é considerada uma classificação, mas uma designação para uma informação de natureza privada, como por exemplo, dados pessoais, significando que a informação é direcionada e que, somente o destinatário e as pessoas autorizadas podem ter acesso a ela;

2. Toda informação deve possuir um rótulo com a sua classificação. As informações não rotuladas devem ser tratadas como “Confidencial”;
3. A classificação das informações deve ser realizada com base nas exigências de negócio do Sociedade, considerando as implicações que seu nível de criticidade trará para o negócio;
4. A classificação das informações deve ser feita para determinar as medidas de proteção necessárias, visando agilizar o processo de tratamento das informações e otimizar os custos com a sua proteção;
5. A classificação deve ser exercida quando a informação é gerada ou adquirida;
6. A informação deve receber tratamento adequado à sua classificação durante todo o seu ciclo de vida;
7. A inexistência de classificação explícita não exime quem a utiliza e gera quanto a avaliar o nível de sensibilidade da informação;
8. Um conjunto de ativos assume automaticamente a classificação mais restrita atribuída a um dos ativos que compõem o conjunto;
9. É expressamente proibida aos colaboradores a utilização, repasse e/ou divulgação indevida de toda e qualquer informação de propriedade da Instituição;
10. Toda divulgação de informação deve ser autorizada. As informações a serem divulgadas interna ou externamente, devem ser cuidadosamente avaliadas quanto à importância e aos possíveis impactos negativos nos negócios, especialmente as que tenham como destinatário o público externo;
11. Antes que informações custodiadas ou de propriedade da Instituição sejam disponibilizadas a terceiros, para qualquer finalidade, deverão ser assegurado que esses terceiros tenham condições de manter sua integridade e confidencialidade;
12. Terceiros devem ser orientados e supervisionados quanto aos aspectos da segurança da informação. O contratante deve garantir que o compromisso de sigilo seja parte integrante do contrato;
13. Informações Internas ou Confidenciais não devem ser descartadas como lixo comum. Documentos impressos ou em mídia eletrônica, que contenham informação com esses níveis de classificação, devem ser destruídos antes de serem descartados, de forma que torne impossível a sua recuperação.

6.5.15. Gestão de incidentes de segurança da informação

Todos os Colaboradores devem reportar imediatamente quaisquer incidentes de segurança que tomarem conhecimento à liderança da área de Segurança da Informação, para que estes possam ser classificados, analisados, monitorados, comunicados e devidamente tratados conforme seu nível de criticidade.

Na ocorrência de incidente envolvendo dados pessoais, a área de Segurança Cibernética deverá acionar, por sua vez, o Encarregado, para que este tome todas as providências. Adicionalmente, em relação ao processo de Tecnologia da Informação, é preciso ainda assegurar que os incidentes e riscos deles decorrentes sejam categorizados e tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar eventuais impactos negativos sobre os sistemas e ativos de informação.

Os procedimentos envolvidos devem descrever o processo de identificação, comunicação do incidente e o processo de investigação do incidente, devem também realizar o recolhimento de evidências e registros para cadeia de custódia. O processo de gerenciamento de incidente deve:

1. Consolidar eventos (trilha de auditoria), identificar e tratar casos que possam afetar a confidencialidade, integridade e disponibilidade dos ativos de informação da empresa.
2. Garantir a detecção de eventos e tratamento adequado, sobretudo na categorização destes como incidentes de segurança da informação ou não.
3. Garantir que incidentes de segurança da informação sejam identificados, avaliados e respondidos da maneira mais adequada possível.
4. Minimizar os efeitos adversos de incidentes de segurança da informação (tratando-os conforme sua criticidade).
5. Reportar as vulnerabilidades de segurança da informação no Comitê de Segurança da Informação e Privacidade, além de tratá-las adequadamente.
6. Ajudar a prevenir futuras ocorrências, através da manutenção de uma base de lições aprendidas (algo parecido com a base dados de erros conhecidos).

   Toda vez que um incidente mal-intencionado for identificado e/ou resolvido, deverá ser feita uma investigação para identificar a origem do ataque e possibilitar a adoção dos procedimentos administrativos e/ou judiciais apropriados.

6.5.16. Treinamento e divulgação

Um programa de conscientização, avaliação, educação e treinamento em Segurança da Informação, com o objetivo de disseminar a cultura de segurança da informação e avaliar o nível de maturidade e conhecimento dos Colaboradores em relação aos temas ministrados, é essencial para garantir os objetivos desta Política.

Todos os Colaboradores e Terceiros contratados da Sociedade devem concluir o treinamento em Segurança da Informação e participarem do programa de educação contínua. Treinamentos adicionais, incluindo treinamentos especializados em segurança, devem ser fornecidos conforme necessário a função e atribuições específicas de cada Colaborador.

Esta Política, juntamente com outras normas e padrões internos de segurança devem ser amplamente divulgadas no processo de admissão e integração de novos Funcionários / Colaboradores, conjuntamente pelas áreas de Recursos Humanos e Segurança da Informação.

6.5.17. Desenvolvimento seguro e segurança nas aplicações

Todo o ciclo de vida do desenvolvimento dos softwares deve seguir as melhores práticas de desenvolvimento a fim de produzir softwares seguros, buscando mitigar o surgimento de vulnerabilidades de segurança. Todo desenvolvimento ou manutenção de software devem ser formalmente autorizados e deve ser realizada uma análise de impacto.

Alterações de escopo de desenvolvimento ou manutenção de software deve ser documentada e formalmente autorizada.

Uma metodologia padronizada de desenvolvimento seguro de aplicações deve ser aplicada no desenvolvimento de novos sistemas ou na manutenção evolutiva de sistemas já existentes.

Controles adequados e trilhas de auditoria ou de registro de atividade devem ser projetados para cada aplicação. Estes controles incluem, mas não estão limitados a validação das entradas, processamento, preparação das saídas e, onde aplicável, à transmissão de dados.

Todas as ferramentas de desenvolvimento devem ser homologadas e licenciadas. O projeto de software deve conter um documento de especificação de segurança que descreva seus objetivos de segurança.

6.5.18. Aquisição, desenvolvimento e manutenção de sistemas

Todo sistema de propriedade da Sociedade, seja ele adquirido ou desenvolvido internamente, deve ser submetido a um processo de avaliação de riscos antes de sua implantação, de forma a garantir seu alinhamento com as práticas de Segurança da Informação estabelecidas nesta Política.

Antes da implantação do aplicativo, todos os dados de teste e quaisquer contas especiais configuradas para fins de teste devem ser removidos. Além disso, todas as contas, nomes de usuário e senhas de aplicativos personalizados devem ser removidos antes que os aplicativos se tornem ativos ou disponíveis para os clientes.

Os desenvolvedores devem estar familiarizados e seguir diretrizes de codificação seguras, como as diretrizes do Open Web Application Security Project (OWASP). É necessário que os desenvolvedores sejam treinados e participem de formações de codificação segura fornecidas uma ou mais vezes por ano. Todas as vulnerabilidades comuns de codificação nos processos de desenvolvimento de software devem ser evitadas.

Os controles de acesso devem estar em vigor para fornecer uma separação distinta. Os ambientes de teste e desenvolvimento devem ser separados do ambiente de produção.

6.5.18.1. Contratação de Serviços de Processamento e Armazenamento de Dados e deComputação em Nuvem (Cloud)

A Sociedade deve assegurar que suas Políticas, estratégias e estruturas para gerenciamento de riscos previstas na regulamentação em vigor, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços, contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior.

Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que contemplem:

1. Adoção de práticas de governança corporativa e de gestão proporcionais à relevância doserviço a ser contratado e aos riscos a que estejam expostas;

2. Verificação da capacidade do potencial prestador de serviço de assegurar:

a. O cumprimento da legislação e da regulamentação em vigor;

b. O acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c. A confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

d. A sua aderência a certificações exigidas pela unidade de negócio regulada pelo BACEN para a prestação do serviço a ser contratado;

e. O acesso da unidade de negócio contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos

aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

f. O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g. A identificação e a segregação dos dados dos clientes da unidade de negócio por meio de controles físicos ou lógicos;

h. A qualidade dos controles de acesso voltados à proteção dos dados e das informaçõesdos clientes da Sociedade.

Na avaliação da relevância do serviço a ser contratado, a unidade de negócio contratante deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado, levando em conta, inclusive, a classificação de risco realizada e respectiva gestão dos serviços a serem contratados.

No caso da execução de aplicativos por meio da internet, a unidade de negócio deve assegurar que o potencial prestador dos serviços adote controles que mitigam os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

Os serviços de computação em nuvem deverão abranger a disponibilidade à unidade de negócio contratante, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

1. Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursoscomputacionais que permitam à unidade de negócio contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos por ela ou adquiridos por terceiros;
2. Implantação ou execução de aplicativos desenvolvidos pela unidade de negócio contratanteou adquiridos por terceiros, utilizando recursos computacionais do prestador de serviços;
3. 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 unidade de negócio é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser previamente comunicada pela unidade de negócio ao BACEN no mínimo, sessenta dias antes da contratação dos serviços e as alterações contratuais que impliquem modificação das informações, no mínimo, sessenta dias antes da alteração contratual.

A comunicação deve conter as seguintes informações:

1. Denominação da empresa a ser contratada;
2. Serviços relevantes a serem contratados;
3. Indicação dos países e das regiões em cada país onde os serviços poderão ser prestados eos dados poderão ser armazenados, processados e gerenciados, no caso de contratação no exterior.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior deve observar os seguintes requisitos:

1. Existência de convênio para troca de informações entre o BACEN e às autoridades supervisoras dos países onde os serviços poderão ser prestados;
2. A unidade de negócio contratante deve assegurar que a prestação dos serviços não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do BACEN;
3. A unidade de negócio contratante deve definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
4. A unidade de negócio contratante deve prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.
5. No caso de inexistência de convênio, a unidade de negócio contratante deverá solicitar autorização do BACEN para a contratação na forma determinada acima.

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

1. Indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
2. Adoção de medidas de segurança para a transmissão e armazenamento dos dados;
3. Manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;
4. Obrigatoriedade, em caso de extinção do contrato, de:
    a. Transferência dos dados citados ao novo prestador de serviços ou à instituição contratante;
    b. Exclusão dos dados citados pela empresa contratada substituída, após a transferência dos dados prevista a confirmação da integridade e da disponibilidade dos dados recebidos;
5. Acesso pela unidade de negócio contratante às informações fornecidas pela empresa contratada, certificações e aos relatórios de auditoria especializada, informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
6. Obrigação da contratada em notificar a unidade de negócio contratante sobre a subcontratação de serviços relevantes e a permissão de acesso do BACEN aos contratos e aos acordos firmados para a prestação de serviços, cópias de segurança dos dados e das informações, bem como adoção de medidas pela unidade de negócio contratante, em decorrência de determinação do BACEN;
7. Obrigação da contratada manter a unidade de negócio 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 deve prever, para o caso da decretação de regime de resolução da unidade de negócio contratante pelo BACEN:

1. 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 referentesaos 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 que estejam em poder da empresa contratada;

2. Obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção dea empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

   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. Notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

Para as relações entre Sociedade e contratados, deve ser elaborado um "Termo Mínimo de Requerimento de Segurança" ("TERMO"), documento que integra, vincula e obriga a parte contratada, e eventual(is) subcontratada(s) e/ou subordinada(s), às disposições da Resolução 4893/21 e da Circular 3909/18, para fins de atendimento da regulação no âmbito do Sistema Financeiro Nacional ("SFN"), que disciplina quanto à elaboração de política de segurança cibernética e, também, sobre a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras.

Por meio do TERMO, a parte contratada, e eventual(is) subcontratada(s) e/ou subordinada(s), (i) ficam sujeitas à supervisão do BACEN, nos termos da Lei nº. 4.595|64, (ii) garantem a conservação do sigilo bancário, por força da Lei Complementar nº. 105, de 10 de janeiro de 2001, ("LC 105/01"), e (iii) comprometem-se a assegurar o acesso às informações requeridas pelo BACEN quando diante dos cenários (iii.1) de Regime de Administração Especial Temporária ("RAET"), do Decreto-Lei nº. 2.321|87 e (iii.2) de intervenção ou de liquidação extrajudicial da instituição financeira Contratante, nos termos da Lei nº. 6.024|74, para os itens (iii.1) e (iii.2) definidos aqui como "Regime de Resolução Bancária".

O TERMO é parte integrante da presente Política, e contempla as ações definidas a serem implementadas pela Contratante e/ou pela parte Contratada, e eventual(is) subcontratada(s) e/ou subordinada(s), para o cumprimento dos requisitos mínimos de governança cibernética no âmbito do gerenciamento de risco operacional da Sociedade.

6.5.19. Registro e monitoramento

A Sociedade deve criar, proteger, monitorar e manter registros (logs) de eventos, a fim de acompanhar e analisar possíveis violações da segurança.

Todas as transações relacionadas aos clientes devem gerar trilhas de auditoria (logs), que deverão ser mantidas de acordo com as legislações vigentes, protegido contra acessos não autorizados.

Não deve haver nenhuma modificação na integridade das trilhas de auditoria (logs), ou seja, não pode haver usuários com permissão de alteração.

Todo acesso de consulta, cópia ou tentativa de modificação e exclusão das trilhas de auditoria (logs) deve ser registrado.

As falhas nos registros das trilhas de auditoria (logs) devem ser registradas, analisadas e devem ser tomadas providências para corrigir o erro de forma imediata.

6.5.20. Avaliação periódica

A Sociedade deve avaliar periodicamente as práticas de Segurança Cibernética e da Informação de forma a aferir a conformidade das ações de seus Funcionários / Colaboradores em relação ao estabelecido nesta Política e na legislação aplicável.

6.5.21. Monitoramento

A Sociedade deve monitorar o acesso e a utilização de seus recursos físicos e tecnológicos, como dos ambientes, equipamentos e sistemas tecnológicos, de forma que ações indesejáveis ou não autorizadas sejam detectadas proativamente.

6.5.22. Revisão e análise crítica

O conjunto de documentos que compõem a Política de Segurança Cibernética e da Informação da Sociedade deve passar por revisões e análises críticas periódicas, legais, estatutários, regulamentares e contratuais que possam influenciar ou afetar o processo de gestão de Segurança da Informação.

6.5.23. Relatório anual e documentação mínima a ser arquivada

Em atendimento à Resolução BCB nº 3.909, anualmente, até o 31 de março, a Sociedade deverá emitir um relatório sobre a implementação do plano de ação de respostas a incidentes, com data base de 31 de dezembro do ano anterior ao relatório, contendo:

1. A efetividade da implementação das ações a serem desenvolvidas pela Instituição para adequar suas estruturas aos princípios e às diretrizes desta Política;
2. 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;
3. Os incidentes relevantes ocorridos no período;
4. Resultado dos testes de continuidade de negócios.
5. Ainda, devem ficar à disposição do BACEN pelo prazo de 05 (cinco) anos:
6. A presente Política, em sua versão mais atualizada;
7. Ata da Reunião do Comitê que aprovou a Política;
8. Documento relativo ao plano de ação e de resposta a incidentes;
9. Relatório anual;
10. Documentação sobre os procedimentos adotados em casos de contratação de serviços relevantes de processamento e armazenamento em nuvem, em atenção ao art. 12, §2º, da Resolução BCB 3.909;
11. Documentação que comprove a adoção dos requisitos relativos à contratação de serviços relevantes de processamento e armazenamento em nuvem prestados no exterior, em atenção ao art. 16, §3º, da Resolução BCB 3.909;
12. Contratos de prestação de serviços relevantes de processamento e armazenamento em nuvem.
13. Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle que visam assegurar a implementação e a efetividade das diretrizes contidas nesta Política.

6.5.24. Conflitos

Na existência de conflito entre os controles de Segurança da Informação e uma necessidade de negócio específica, controles mitigatórios devem ser analisados e implementados a fim de viabilizar os objetivos da Sociedade, havendo ainda a necessidade de registro da aceitação dos riscos remanescentes por parte da Diretoria.

6.6. Responsabilidades

6.6.1. Diretoria

1. Aprovar esta Política de Segurança Cibernética e da Informação;
2. Prover os recursos humanos, materiais e financeiros necessários à Segurança da Informação e acompanhar periodicamente a evolução dos indicadores e resultados das medidas de segurança implementadas;
3. Assegurar que esta Política e as diretrizes de Segurança da Informação estão estabelecidas esão compatíveis com a direção estratégica da Instituição, assim como zelar pelo seu estrito cumprimento;
4. Prover comprometimento e apoio à aderência a esta Política de acordo com os objetivos e estratégias de negócio estabelecidas;
5. Fornecer as áreas de Tecnologia da Informação e Segurança da Informação amplo apoio e recomendação sempre que necessário, permitindo a melhoria contínua da estratégia de Segurança da Informação

6.6.2. Segurança da Informação

1. Assegurar a divulgação desta Política a todos os Funcionários / Colaboradores, Terceiros e demais partes interessadas, inclusive suas atualizações, realizar treinamentos periódicos de conscientização sobre os procedimentos e controles de segurança aqui previstos;
2. Gerir a segurança da informação criando e acompanhando os indicadores de performance e eficiência;
3. Gerir os projetos de segurança da informação;
4. Avaliar os controles de segurança dentro do seu escopo de ação;
5. Desenvolver programas de conscientização e educação em segurança da informação;
6. Garantir a realização de testes de invasão e investigações no ambiente periodicamente.
7. Avaliar e responder aos incidentes relacionados a processos e pessoas;

6.6.3. Tecnologia da Informação

1. Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantesde hardware e software;
2. Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia;
3. Conduzir a gestão dos acessos a sistemas e informações da Sociedade;
4. Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos detecnologia da informação;
5. Informar imediatamente a área de Segurança da Informação, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos;
6. Controlar alterações em ativos de TI e garantir que estas sejam analisadas criticamente e testadas para que não ocorram impactos adversos na operação ou em sua segurança;
7. Garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio;

8. Garantir que todos os ativos críticos de tecnologia da informação devem ser instalados em ambientes especializados. Estes devem conter todas as proteções e contingências necessárias para a sua respectiva proteção;
9. Adequar esta Política às novas tecnologias que vierem a ser adotadas pela Instituição, de forma a mantê-la sempre abrangente e atualizada.

6.6.4. Comitê de Segurança da Informação e Cibernética e Privacidade

1. Aprovar a realização de investigações e determinar a adoção de medidas necessárias.
2. Assegurar que as infrações e violações sejam seguidas de ações disciplinares aplicáveis.
3. Tomar ciência de riscos corporativos;
4. Assegurar a conformidade de rotinas, práticas e procedimentos;
5. Apreciar os relatórios emitidos pelos Órgãos Reguladores e Auditorias;
6. Acompanhar a efetividade e eficácia das atividades e ações relacionadas aos temas;
7. Assegurar que Conselho esteja ciente dos assuntos que possam causar impacto significativo àimagem;
8. Deliberar sobre estratégias e contratação de serviços especializados.

6.6.5. Recursos Humanos

1. Garantir que todos os novos Colaboradores leiam, entendam e declaram estarem cientes acerca da presente Política e de suas diretrizes;
2. Comunicar prontamente as áreas de Tecnologia da Informação e Segurança da Informação toda e qualquer alteração no quadro de pessoal, incluindo demissões, alterações de cargos, funções, entre outros necessários a fim de evitar acessos não autorizados e/ou em níveis não condizentes com a função ou cargo exercido.
3. Garantir que todos os contratos de trabalho de colaboradores contenham as cláusulas pertinentes às responsabilidades dos funcionários pela segurança da informação e confidencialidade.
4. Sempre que terminar a colaboração de um funcionário a área de recursos humanos deverá recolher os recursos disponibilizados e informar a área de infraestrutura para que esse colaborador possa ser, o mais rapidamente possível, desativado e os seus acessos cancelados.

6.6.6. Riscos, Controles e Compliance

1. Apoiar as áreas de Tecnologia da Informação e Segurança da Informação em investigações envolvendo incidentes de segurança e garantir a aplicação das sanções administrativas e judiciais cabíveis previstas em políticas internas e em lei.

6.6.7. Funcionários / Colaboradores e Terceiros Contratados

1. Ler atentamente esta Política, declarar ciência e aderir às diretrizes que constam neste documento;
2. Utilizar as ferramentas e Ativos que lhe forem colocadas à disposição pela de forma diligente eem estrita conformidade com as políticas e normas internas, incluindo esta Política.
3. Prover segurança às informações utilizadas no relacionamento com terceiros, obedecendo aosrequisitos contratuais e/ou legais;
4. Administrar de forma conveniente e adequada, sob a ótica da segurança e proteção,

informações, ativos de sistemas de informação e mídias que contenham qualquer informação pertencente ou custodiada;

5. Conhecer o tema de segurança da informação, com o intuito de evitar a ação de quaisquer tipos de fraudadores, ou ser vítima destes;
6. Guardar sigilo sobre qualquer informação que ainda não tenha sido divulgada, obtida em razão do cargo e capaz de influir de modo ponderável no negócio, sendo-lhe vedado valer-se da informação para obter vantagem para si ou para outrem;
7. Zelar para que os aspectos de segurança da informação sejam respeitados, inclusive comunicando à empresa situações suspeitas ou efetivamente irregulares;
8. Participar dos treinamentos e conscientização sobre práticas de Segurança da Informação quevenham a ser oferecidos pela Instituição;
9. Reportar as áreas de Tecnologia da Informação e Segurança da Informação toda e qualquer suspeita de violação às diretrizes, procedimentos e controles previstos nesta Política;
10. Devolver (ou destruir, caso assim expressamente solicitado pela área de Segurança da Informação) todas as informações que estejam em seu poder ao final do seu vínculo com a Sociedade.

6.7. Penalidades

Os colaboradores que não observarem as diretrizes e as obrigações dessa política, incluindo parceiros, colaboradores, prestadores de serviço terceirizado e fornecedores, por negligência, culpa ou dolo, estão sujeitos a ações disciplinares, incluindo a rescisão do contrato e/ou medidas administrativas ou criminais, além das penalidades previstas em lei.

7. VIGÊNCIA

Este **IN** entra em vigor na data de sua publicação, e vigorará por prazo indeterminado, devendo ser atualizada sempre que a área responsável entender necessário ou quando da ocorrência de alterações da regulação | legislação pertinente.

8. HISTÓRICO DAS REVISÕES

Versão	Aprovador	Data de Revisão	Descrição
1ª versão	Diretoria	14/10/2022	
2ª versão	Diretoria	17/07/2023	

9. ANEXOS

Sequencial	Título

10. APROVAÇÃO

Órgão Aprovador | Diretoria	
Membro	**Assinatura**
Henrique Fernando Lucas	
Camila Dias Barros	
Alexandra Oliveira	

Página de assinaturas

Alexandra Oliveira
913.465.766-53
Signatário

Henrique Lucas
013.739.756-95
Signatário

Camila Barros
014.750.386-82
Signatário

HISTÓRICO

27 jul 2023 13:32:39 — **Alexandra Eliane dos Santos Oliveira** criou este documento. (E-mail: alexandra.oliveira@cdcbank.com.br, CPF: 913.465.766-53)

27 jul 2023 14:35:13 — **Camila Dias Barros** *(E-mail: camila.barros@cdcbank.com.br, CPF: 014.750.386-82)* visualizou este documento por meio do IP 177.26.89.157 localizado em Rio de Janeiro - Rio de Janeiro - Brazil

27 jul 2023 14:35:13 — **Camila Dias Barros** *(E-mail: camila.barros@cdcbank.com.br, CPF: 014.750.386-82)* assinou este documento por meio do IP 177.26.89.157 localizado em Rio de Janeiro - Rio de Janeiro - Brazil

27 jul 2023 13:50:06 — **Henrique Fernando Lucas** *(E-mail: henrique.lucas@cdcbank.com.br, CPF: 013.739.756-95)* visualizou este documento por meio do IP 177.26.80.128 localizado em Rio de Janeiro - Rio de Janeiro - Brazil

27 jul 2023 13:50:06 — **Henrique Fernando Lucas** *(E-mail: henrique.lucas@cdcbank.com.br, CPF: 013.739.756-95)* assinou este documento por meio do IP 177.26.80.128 localizado em Rio de Janeiro - Rio de Janeiro - Brazil

27 jul 2023 13:32:39 — **Alexandra Eliane dos Santos Oliveira** *(E-mail: alexandra.oliveira@cdcbank.com.br, CPF: 913.465.766-53)* visualizou este documento por meio do IP 200.233.160.81 localizado em Ribeirão das Neves - Minas Gerais - Brazil

27 jul 2023 13:32:45 — **Alexandra Eliane dos Santos Oliveira** *(E-mail: alexandra.oliveira@cdcbank.com.br, CPF: 913.465.766-53)* assinou este documento por meio do IP 200.233.160.81 localizado em Ribeirão das Neves - Minas Gerais - Brazil