Data de Emissão 23/07/2021	Credifisco	Versão 1ª

Documento

8. 5 Política de Segurança Cibernética

1. OBJETIVO

Atendendo ao Art. 3 Inciso I. Esta política tem por objetivo atender a resolução CMN 4893 sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

2. INTRODUÇÃO

Para a elaboração desta Política, foi considerado o porte, o perfil de risco, o modelo de negócio, a natureza das operações, a complexidade dos produtos, serviços, atividades e processos, bem como a sensibilidade dos dados e das informações sob responsabilidade da Credifisco.

3. DIRETRIZES

Cabe à Administração garantir a implementação, gestão, manutenção e conscientização deste conteúdo a todos os colaboradores e prestadores de serviços da Cooperativa.

Cabe a todos os colaboradores e prestadores de serviços a responsabilidade em executar suas atividades conforme diretrizes estipuladas nesta política.

A presente política apresenta os principais procedimentos e controles.

As atividades sempre geram um protocolo com a nomenclatura PCXXX, e seguem de acordo com a tabela abaixo:

Mensal	Análise de logs File Server (Cota de arquivos, antivírus, desligamentos bruscos, auditoria de pastas, limpeza de perfis, updates, etc).	Verificar console de servidor tendo atenção para pacotes de atualização do antivírus, logs de desligamento do equipamento, estrutura de pastas. Rodar update de windows server, validar usuários/arquivos e pastas atualizadas.
Mensal/Semanal	Análise de Firewall (Firmwares disponíveis, logs de acessos, dashboards)	Gerenciamento semanal de console que permite coletar dados de ameaças, ataques contra rede interna
Mensal	Avaliação de log de quedas, servidor e Firewall	Analisar console de firewall, sendo este agendamento contribuinte para a manutenção correta do equipamento. Atualização de firmwares disponíveis e estáveis.

Os procedimentos e os controles devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros, na adoção de novas tecnologias empregadas nas atividades da Cooperativa, incluindo controles específicos voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis.

Cabe à Cooperativa o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Credifisco, considerando, inclusive, plano adequado de continuidade de negócios.

O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

É necessário criar iniciativas para compartilhamento de informações sobre os incidentes relevantes, com as demais instituições financeiras autorizadas a funcionar pelo Banco Central do Brasil.

O gerenciamento de riscos deve dispor, no que se refere à continuidade de negócios, sobre o tratamento dos incidentes relevantes relacionados com o ambiente cibernético.

A Credifisco 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. Sendo assim, para reduzir a vulnerabilidade da cooperativa a incidentes cibernéticos e atender aos demais objetivos de segurança cibernética, são adotados procedimentos e controles, conforme porte e perfil de risco, considerando:

a) Regras para controlar complexidade e qualidade das credenciais utilizadas para acesso aos sistemas e aos dados sob responsabilidade da cooperativa;

b) Recursos criptográficos adequados para garantir a privacidade, integridade e não-repúdio dos dados mantidos;

c) Solução de proteção contra ameaças avançadas em e-mail e no acesso a sites na internet, solução de proteção de dispositivos, antivírus de borda;

d) Manutenção de cópias de segurança dos dados e das informações.

e) Implantação e manutenção de firewall para proteção a ataques cibernéticos; e

f) Gestão de acesso.

Os procedimentos e controles são aplicados para sistemas de informação desenvolvidos internamente ou adquiridos de terceiros.

As diretrizes destacadas contemplam procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria Cooperativa.

A Credifisco estabeleceu plano de ação e de resposta a incidentes, documento PLANO_ACAO_INCIDENTES_PSCI.YYYYMM.

As informações de propriedade ou sob custódia da Credifisco, mantidas em meio eletrônico ou físico, são classificadas de acordo com os requisitos de proteção esperados em termos de sigilo, valor, requisitos legais, sensibilidade e necessidades do negócio, de modo que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, conforme diretrizes de classificação da informação estipuladas na presente política.

São adotados mecanismos para disseminação da cultura de segurança cibernética na Cooperativa, incluindo a prestação de informações a associados e usuários sobre precauções na utilização de produtos e serviços financeiros. Como principais mecanismos para disseminação da cultura de segurança cibernética, destacam-se:

a) a implementação de programas de capacitação e de avaliação periódica de pessoal;

b) a prestação de informações a cooperados e usuários sobre precauções na utilização de produtos e serviços financeiros;

c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética;

d) Divulgação da Política de Segurança Cibernética para funcionários da Cooperativa e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações. A Credifisco também deve divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética.

Para as ações de divulgação, a Cooperativa tem o dever de garantir a educação e a conscientização de empregados, terceiros contratados e, quando cabível, de associados, sobre as práticas de Segurança da Informação adotadas pela Credifisco.

Deve ser divulgada a todos os colaboradores da Credifisco em linguagem compatível com as funções que desempenham e em proporção à sensibilidade das informações que utilizam em seu cotidiano e disposta de maneira que seu conteúdo

possa ser consultado a qualquer momento e seja protegido contra alterações. O público geral deve ter acesso a um resumo da política de segurança da informação. O conteúdo deste resumo, acessível pelo público geral, deve ser autorizado pelo Conselho de administração.

Funcionários

E-mail

Cartilha no drive

Política impressa e disponível para consulta

Política digitalizada e disponível para consulta

Assinatura do Termo de Ciência

Prestadores de Serviços

E-mail

Assinatura do Termo de Ciência

Público em geral

- Resumo da política disponível no site da Credifisco para download

Complementam esta política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a segurança cibernética da cooperativa.

Os documentos complementares tratam sobre cenários de incidentes considerados nos testes de continuidade de negócios, definição de procedimentos e de 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 Credifisco, e definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes.

A Cooperativa deve designar diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

O diretor designado pode desempenhar outras funções na Cooperativa, desde que não haja conflito de interesses. Suas principais atribuições e responsabilidades são:

a) Supervisionar o desenvolvimento, a implementação e o desempenho da estrutura de gerenciamento de segurança cibernética, incluindo seu aperfeiçoamento;

b) Fazer recomendações de aperfeiçoamento da política, planos, manuais, controles e procedimentos relacionados à segurança cibernética;

c) Implementar e executar os procedimentos descritos nas políticas, planos e manuais relativos ao tema;

d) Subsidiar e participar do processo de tomada de decisões estratégicas relacionadas ao gerenciamento de segurança cibernética;

e) Providenciar o relacionamento com órgãos de supervisão internos e externos;

f) Compartilhar informações sobre incidentes cibernéticos relevantes com as instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

A Diretoria é responsável por:

a) Definir políticas, planos, manuais e controles, assim como, revisar e aprovar periodicamente as políticas e estratégias de gerenciamento de segurança cibernética;

b) Assegurar a aderência às políticas e às estratégias de gestão de segurança cibernética;

c) Assegurar a correção tempestiva das deficiências das estruturas de gerenciamento de segurança cibernética;

d) Promover a disseminação da cultura de gerenciamento de segurança cibernética.

A Credifisco deve elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, contendo: (i) a efetividade da implementação das ações desenvolvidas para adequar a estrutura organizacional e operacional da Cooperativa, 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 desta política; (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.

O relatório deve ser apresentado ao Conselho de Administração até 31 de março do ano seguinte ao da data base.

A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo anualmente, e aprovados pelo conselho de administração da Credifisco.

A Credifisco deve assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos previstas nos normativos vigentes, 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, a Cooperativa deve adotar procedimentos documentados que contemplem a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas, e a verificação da capacidade do potencial prestador de serviço, conforme artigo 12 da Resolução CMN nº 4893 de 26 de Fevereiro de 2021.

De forma conjunta a este processo, a Credifisco dispõe de documentos internos sobre Diretrizes e Requisitos para Contratação de Serviços de TI, bem como Critérios de Decisão para Contratação de Serviços de TI, que devem ser

considerados para a avaliação e contratação de prestador de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem.

Além disso, para a contratação e gestão de fornecedores, a Cooperativa deve garantir que todo serviço de TI deve ser classificado com base em uma análise de risco para se definir a sua criticidade e, assim se avaliar a possibilidade de sua prestação por uma empresa terceira.

Serviços críticos deverão sempre requerer uma homologação prévia do fornecedor, para garantir riscos mínimos com relação a sua prestação no que se refere a segurança e privacidade de dados.

Por isso, a Credifisco deve estabelecer em contrato requisitos mínimos de segurança e privacidade de dados que devem ser cumpridos pelo prestador de serviço.

Devem ser verificados, de forma regular, os requisitos de segurança e privacidade de dados de fornecedores críticos conforme definidos nas cláusulas contratuais estabelecidas entre as partes.

O gerenciamento de fornecedores deverá considerar a avaliação de risco e classificação dos fornecedores (estratégico, tático, operacional e base), sendo: (i) Estratégicos: Contratos de parceria, envolvendo compartilhamento de informações também estratégicas; (ii) Táticos: Contratos de atividade Comercial, com significante interação com a Cooperativa; (iii) Operacional: Fornecedores operacionais; e (iv) Base: Fornecedores que geram pouco valor a CREDIFISCO. Ex. Distribuidor de materiais de limpeza, papelaria etc.

Deve ser medido, de forma regular, o desempenho dos fornecedores críticos quanto ao cumprimento das metas acordadas e os resultados avaliados. Os

resultados devem ser discutidos com o fornecedor para se identificar as necessidades e oportunidades de melhoria.

Cada fornecedor deverá ter um gestor designado que acompanha o seu desempenho, tornando-o responsável pela qualidade dos serviços fornecidos. Atualmente a cooperativa está estruturada desta maneira. Nomeando os donos de processos e fornecedores.

Ex. Responsável pela Contabilidade, responsável pelo Mantenedor de Telefonia, responsável pelo Mantenedor do software Omnichanel, este certamente é responsável por cumprir o acordo/contrato firmado entre as partes.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada ao Bacen, até dez dias após a contratação dos serviços ou alterações contratuais que impliquem modificação das informações, considerando: (i) a denominação da empresa contratada; (ii) os serviços relevantes 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.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior deve observar os seguintes requisitos descritos no Artigo 16 da Resolução CMN nº 4893 de 26 de fevereiro de 2021.

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever os itens destacados no artigo 17 da Resolução CMN nº 4893 de 26 de fevereiro de 2021.

A Credifisco deve assegurar que sua política para gerenciamento de riscos disponha, no que se refere à continuidade de negócios, sobre o tratamento dos incidentes relevantes relacionados com o ambiente cibernético, considerando o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Cooperativa.

Além disso, a política também deve contemplar que os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, contenha cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da Cooperativa.

Devem ser contemplados, também, os cenários de incidentes considerados nos testes de continuidade de negócios.

Ainda no tocante à continuidade de negócios, a Cooperativa deve adotar procedimentos para o gerenciamento de riscos, considerando:

a) o tratamento previsto para mitigar os efeitos dos incidentes relevantes para as atividades da Cooperativa e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados;

b) o prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos, relacionados com o ambiente cibernético; e

c) a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes relacionados com o ambiente cibernético que configurem uma situação de crise pela Credifisco, bem como das providências para o reinício das suas atividades.

d) Estabelecer e documentar os critérios que configurem uma situação de crise para a Credifisco.

A Cooperativa deve instituir e cumprir mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade desta política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo:

I - A definição de processos, testes e trilhas de auditoria;

II - A definição de métricas e indicadores adequados; e

III - A identificação e a correção de eventuais deficiências.

Atualmente, todo atendimento é gerado um ticket ao Contratante. Após, é realizada a atividade com as evidencias técnicas que comprovam sua finalização. Esta ferramenta permite relógios para controle das atividades aqui descritas x com o que foi contratado.

Quanto aos fornecedores, a Credifisco possui um checklist para contratação de fornecedores.

As notificações recebidas sobre a subcontratação de serviços relevantes também devem ser consideradas na definição dos mecanismos de acompanhamento.

Os mecanismos devem ser submetidos a testes periódicos pela auditoria interna, quando aplicável, compatíveis com os controles internos da Cooperativa.

A Credifisco se compromete com iniciativas para o compartilhamento de informações sobre os incidentes relevantes. As informações compartilhadas devem ficar à disposição do Bacen.

A presente Política de segurança cibernética e da informação visa prover diretrizes para a segurança da informação, relacionadas ao manuseio, controle, proteção (contra indisponibilidade, divulgação imprópria, acesso indevido e modificação não autorizada de informações e de dados) e descarte;

a) é elaborada, aprovada e revisada periodicamente pela Diretoria da Credifisco;

b) é aplicável às informações armazenadas ou em trânsito;

c) é observada por todos os usuários que compõem a estrutura organizacional da Credifisco e pelas demais pessoas com acesso autorizado às informações;

d) tem o cumprimento acompanhado pela Diretoria;

e) é normatizada e divulgada aos empregados e a qualquer pessoa que mantenha relação de prestação de serviço com a Credifisco.

Para acessar os aplicativos corporativos disponibilizados pela Credifisco, o usuário deverá estar identificado, autenticado e autorizado. Suas ações poderão ser auditadas a qualquer tempo. Os acessos serão concedidos à medida que solicitados e autorizados pela Diretoria.

Para os contratos firmados com terceiros, a Credifisco inclui cláusulas de confidencialidade, de acordo de nível de serviço e em cumprimento a todas as regras definidas nesta Política e nos documentos a ela subordinados.

A Credifisco aplicará penalidades nos casos de infrações às regras desta Política e dos documentos a ela subordinados, de acordo com o grau de impacto da infração.

Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

1. A presente Política de Segurança Cibernética e da Informação;

2. Plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética;

3. Relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data base 31 de dezembro e aprovação até março do ano seguinte ao da data base;

4. Documentação sobre os procedimentos de que trata o art. 12, § 2º da Resolução CMN nº 4893 de 26 de fevereiro de 2021;

5. Documentação de que trata o art. 16, § 3º da Resolução CMN nº 4893 de 26 de fevereiro de 2021, no caso de serviços prestados no exterior;

6. Contratos de que trata o art. 17 da Resolução CMN nº 4893 de 26 de fevereiro de 2021;

7. Dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle de que trata o art. 21 da Resolução CMN nº 4893 de 26 de fevereiro de 2021;

8. Documentação com os critérios que configurem uma situação de crise de que trata o art. 20, Parágrafo único, da Resolução CMN nº 4893 de 26 de fevereiro de 2021.

- **Tópico:**

4. SEGURANÇA DA INFORMAÇÃO

Este capítulo, juntamente com a política de segurança cibernética e da informação é um mecanismo de segurança essencial, tanto para a cooperativa quanto para os cooperados. Ela visa assegurar a proteção das informações constantes na Cooperativa, em conjunto com o Código de Conduta e Ética, determinando regras e comportamentos a serem seguidos.

Casos de mau comportamento que possibilitem a perda ou o vazamento indevido de informações da CREDIFISCO poderão ser penalizados da forma adequada, de acordo com os danos causados para as partes envolvidas.

Esta Política de Segurança Cibernética e da Informação define regras específicas para acessos, senhas, backup, mecanismos de segurança e uso aceitável.

A presente política também objetiva definir os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza, bem como as penalidades às quais está sujeito, caso não a cumpra.

Para prover aos cooperados a segurança da informação necessária para a privacidade e o sigilo de suas informações, devem-se adotar comportamentos e regras, observando a cultura e outras recomendações da Cooperativa.

Os atributos básicos para a segurança da informação são a confidencialidade, a integridade e a disponibilidade.

- **Objetivos**

Estabelecer diretrizes que permitam aos colaboradores e prestadores de serviços da CREDIFISCO seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Preservar as informações da CREDIFISCO bem como de seus cooperados quanto à:

• **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

• **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

• **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

- **APLICAÇÕES DA Política de Segurança Cibernética**

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Este documento dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu coordenador ou da Diretoria Executiva sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

- **PRINCÍPIOS DA Política de Segurança Cibernética**

Toda informação produzida ou recebida pelos colaboradores da CREDIFISCO como resultado da atividade profissional pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços. A CREDIFISCO, por meio da Diretoria Executiva, poderá solicitar ao prestador de serviços de TI o monitoramento do uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

- **REQUISITOS DA Política de Segurança Cibernética**

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da CREDIFISCO a fim de que a política seja cumprida dentro e fora da Cooperativa. Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da Diretoria Executiva com o apoio do prestador de serviço de TI. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um **Termo de Responsabilidade**.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Coordenador, que neste momento irá solicitar a análise do prestador de serviços de TI; por fim se julgar necessário, **deverá encaminhar posteriormente à Diretoria Executiva**.

Todos os requisitos de segurança da informação, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e

justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a Credifisco julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas desenvolvidos pela Cooperativa ou por terceiros

Esta PSI deve ser seguida independentemente de vínculo empregatício ou prestação de serviço. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da Informação é o ato de atribuir um rótulo à Informação, com base no grau de confidencialidade necessário para proteção da Informação, e servirá como critério para a designação do rótulo classificatório aplicável.

Os rótulos classificatórios determinam o nível de proteção aplicável durante o Ciclo de Vida da Informação, representando o nível de proteção da Informação.

A classificação deve ocorrer somente de acordo com os critérios definidos pela Cooperativa, com base nos possíveis impactos negativos que a Credifisco possa vir a sofrer caso a Informação se torne conhecida por pessoas não autorizadas, independentemente do seu contexto e/ou formato da Informação.

Para a troca de informações, todos os colaboradores da Credifisco deverão observar e aplicar os seguintes rótulos:

“Confidencial”

É o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da Cooperativa. São protegidas, por exemplo, por criptografia. Dados confidenciais devem ser usados quando existe uma pessoa especifica que pode recepcioná-los.

“Restrita”

É o nível médio de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores. Podem ser protegidas, por exemplo, restringindo o acesso à uma pasta ou diretório da rede.

“Uso interno”

Representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da Cooperativa, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

“Pública”

São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público. No entanto, sempre cabe lembrar dos outros dois pilares: a disponibilidade e a integridade.

Para as questões que envolvem a LGPD, os colaboradores devem usar o rótulo **"Dado Pessoal/Sensível"**.

Aos ativos de informação são aplicados requisitos de classificação, de acordo com regras institucionalizadas definidas com base nos aspectos legais e necessidades do negócio.

Todo o acesso às informações e a utilização dos recursos corporativos poderão ser monitorados, não sendo permitido ao usuário o uso desses recursos para atividades que não estejam relacionadas ao exercício das suas funções.

Qualquer acesso à informação será previamente autorizado pela Diretoria, levando em conta estritamente as atividades desenvolvidas pelo usuário dentro da Credifisco. Quando por meio de sistema, o acesso somente será permitido a usuários devidamente autenticados.

Cabe à Diretoria definir as regras para a guarda e preservação das informações conforme o nível de classificação;

As informações produzidas no ambiente da Credifisco, por meio dos recursos próprios ou de serviço contratado, são de propriedade desta e somente poderão ser copiadas, divulgadas, publicadas, com autorização da Diretoria.

Informações confidenciais não serão discutidas em locais públicos ou de circulação de pessoas não ligadas à Credifisco.

6. ACESSO À REDE E GESTÃO DE ACESSOS

A gestão de acessos tem por objetivo estabelecer critérios para acesso aos sistemas eletrônicos utilizados pela Credifisco.

Os colaboradores e terceiros terão acesso apenas aos dispositivos, infraestrutura, sistemas e informações estritamente necessários à realização das tarefas de sua responsabilidade. Todo e qualquer dispositivo, sistema, ou informação acessados poderão ser monitorados e auditados, principalmente objetivando identificar responsáveis por eventuais danos. Toda informação presumir-se-á de propriedade da CREDIFISCO quando se utilizar de sua infraestrutura.

É desejável que a Cooperativa tenha controle de log de acesso.

- **Senhas**

A Política de Senhas define as regras sobre o uso de senhas nos recursos computacionais, como tamanho mínimo e máximo, regra de formação e periodicidade de troca de 3 em 3 meses.

- **Regras**

As senhas de acesso são individuais, intransferíveis, de responsabilidade única e exclusiva do usuário e não podem ser compartilhadas ou divulgadas.

As senhas utilizadas pelos colaboradores da CREDIFISCO devem conter, no mínimo, 8 (oito) caracteres, sendo, no mínimo, 3 (três) letras – ao menos uma letra maiúscula, 3 (três) números, e 1 (um) caractere especial.

As senhas deverão ser alteradas trimestralmente, ou sempre que se possa desconfiar que a senha possa ter sido descoberta, ou que o computador utilizado possa ter sido invadido ou infectado.

Nenhuma senha pessoal deve ser compartilhada com outras pessoas, mesmo que colaboradores, exceto com autorização expressa dos integrantes da Diretoria.

Nenhuma senha poderá conter quaisquer tipos de dados pessoais que possam ser descobertos por engenharia social, como nomes, sobrenomes, números de telefones, datas, entre outros. As senhas também não deverão conter sequências de teclado, como “asd” ou “123”, por serem facilmente observadas durante a digitação.

- **Comportamentos**

Os comportamentos listados abaixo deverão ser adotados pelos colaboradores em relação às senhas que manipulam:

- certificar-se de não estar sendo observado ao digitar as suas senhas;

- não fornecer as suas senhas para outra pessoa, em hipótese alguma;

- certificar-se de fechar a sua sessão (logout) ao acessar sites que requeiram o uso de senhas;

- não usar a mesma senha para todos os serviços que acessa;
- evitar escolher questões de segurança cujas respostas possam ser facilmente adivinhadas;
- certificar-se de utilizar serviços criptografados quando o acesso a um site envolver o fornecimento de senha;
- manter sua privacidade, reduzindo a quantidade de informações que possam ser coletadas sobre você;
- manter a segurança do seu computador;
- ser cuidadoso ao usar a sua senha em computadores potencialmente infectados ou comprometidos.

7. **BACKUP:**

A Política de Backup define regras sobre a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução.

- **Regras**

O backup de todos os diretórios do Active Directory deve ser realizado automaticamente, com periodicidade mensal. As cópias devem identificar o mês de referência, e deverão ficar retidas por, no máximo, 6 (seis) meses no storage.

- **Comportamentos**

Os seguintes comportamentos deverão ser seguidos pela Cooperativa a fim de evitar perda de informações:

- manter backups atualizados, de acordo com a frequência de alteração dos dados;
- manter backups em locais seguros, bem condicionados e com acesso restrito;
- configurar para que backups sejam realizados automaticamente e certificar-se de que eles estejam realmente sendo feitos;
- realizar backups antes de efetuar grandes alterações no sistema ou de enviar o computador para manutenção;
- armazenar dados sensíveis em formato criptografado;
- manter backups redundantes;
- assegurar-se de conseguir recuperar backups;
- manter backups organizados e identificados;

- nunca recuperar um backup se puder conter dados não confiáveis.

Mecanismos de Segurança

A cooperativa deverá manter ferramentas de segurança instaladas e ativas, além de, periodicamente, desinstalar programas não mais utilizados, ou suas versões antigas.

É vedada a instalação, conexão ou utilização de quaisquer dispositivos de armazenamento e conectividade (modem 3G, HD externo, pendrive etc.), salvo os de propriedade da Credifisco ou autorizados pela Diretoria:

a) pertencentes a Credifisco: em ambiente interno e externo à instituição;

b) de terceiros que são utilizados para o trabalho na Credifisco: em ambiente interno à instituição.

c) As instalações que abrigam informações, documentos e equipamentos de processamento de informação sensível têm perímetros de segurança com controles apropriados que garantem o acesso apenas a pessoas autorizadas e possuem mecanismos de prevenção a incêndios e outros tipos de sinistros.

d) Todos os softwares utilizados pela Credifisco são licenciados. Não são instalados, conectados e utilizados softwares não autorizados pela Diretoria, independente da natureza de uso ou aplicação. Os usuários respeitam o direito à propriedade intelectual, na forma da legislação em vigor, não reproduzindo ou divulgando material sem a autorização do autor.

- **Firewall**

A segurança deverá ser reforçada pela instalação de firewall pessoal em cada computador, protegendo-o contra acessos não autorizados vindos da Internet. Todo o tráfego de entrada nos computadores deverá ser bloqueado por padrão, liberando as conexões conforme necessário.

Os logs gerados pelo firewall deverão ser analisados periodicamente, a fim de identificar possíveis problemas de segurança.

- **Antivírus**

Todos os computadores deverão ter antivírus instalados e ativos. A varredura completa deverá ser realizada mensalmente.

Os logs gerados pelo antivírus deverão ser analisados periodicamente, a fim de identificar possíveis problemas de segurança.

- **Critérios de Uso Aceitável**

Os comportamentos abaixo discriminados, quando não autorizados pela Diretoria ou não justificados, estão sujeitos a penalidades dos envolvidos:

- compartilhamento de senhas;
- divulgação de informações confidenciais;
- envio de boatos e mensagens contendo spam e códigos maliciosos;
- envio de mensagens com objetivo de difamar, caluniar ou ameaçar alguém;
- cópia e distribuição não autorizadas de material protegido por direitos autorais;
- ataques a outros computadores;
- comprometimento de computadores ou redes;
- desativação dos mecanismos de segurança.

Outros comportamentos não listados poderão ser penalizados proporcionalmente aos danos causados aos envolvidos e à Cooperativa.

Em complemento a este capítulo, a Cooperativa deve seguir as boas práticas de segurança da informação, conforme documento que orienta e estabelece as diretrizes corporativas da CREDIFISCO para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em

todas as áreas da Cooperativa, este PSI, com a intenção de aumentar a segurança da infraestrutura tecnológica.

O documento deve ser custodiado em pasta disponível File Server juntamente com os procedimentos de TI.

8. DISPOSIÇÕES FINAIS

Este documento foi aprovado pelo Conselho de Administração da Credifisco em reunião de 28/07/2021 e entrará em vigor na data da aprovação em xxxxxx.