Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

CoopCargill

Cooperativa de Economia e Crédito Mútuo dos Funcionários da Cargill

2.7. POLÍTICA DE RISCO CIBERNÉTICO

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

SUMÁRIO

2. GERENCIAMENTO DE RISCOS 3
2.7 Política de Risco Cibernético 3
2.7.1 Abrangência 3
2.7.2 Objetivo 3
2.7.3 Organograma 4
2.7.4 Papéis e Responsabilidades. 4
2.7.4.1. Conselho de Administração 4
2.7.4.2. Diretoria Executiva 5
2.7.4.3. Colaboradores 5
2.7.4.4. Conselho Fiscal 6
2.7.4.5. Cooperados 6
2.7.4.6. Prestadores de Serviços 7
2.7.5 Implementação da Política Cibernética 7
2.7.6 Princípios de Segurança da Informação 7
2.7.7 Controles da Segurança da Informação 9
2.7.8 Registros de Incidentes Relevantes 9
2.7.9 Divulgação da Política de Risco Cibernético 10
2.7.10 Plano de Ação e de Respostas à Incidentes 11
2.7.11 Avaliação e Contratação de Serviços de TI e de Processamento, Armazenamento de Dados e de Computação em Nuvem 11
2.7.12 Responsabilidade entre a COOPCARGILL e a mantenedora Grupo Cargill Agrícola S/A.... 13
2.7.13 Relatórios de testes de Segurança na Informação..... 14
2.7.14 Continuidade dos Negócios..... 15
2.7.15 Reporte/Comunicação à Diretoria Executiva 15
2.7.16 Comunicações ao Banco Central do Brasil. 15
2.7.17 Considerações Finais 16
2.7.18 ANEXO I - Termo de Compromisso da Política e Segurança da Informação. 17
2.7.19 ANEXO II Relatório de Incidente de Segurança da Informação 18

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

2. GERENCIAMENTO DE RISCOS

2.7 Política de Risco Cibernético

Esta Política de Risco Cibernético atende à Resolução Conselho Monetário Nacional - CMN nº 4.893/21 que 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 a serem observados pela **Cooperativa de Economia e Crédito Mútuo dos Funcionários da Cargill – COOPCARGILL**.

Esta política tem por objetivo estabelecer os princípios, conceitos, valores e práticas sobre os requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, que devem ser adotados pelos administradores e colaboradores da **COOPCARGILL,** buscando assegurar confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Os computadores e redes utilizados são da empresa mantenedora **Grupo Cargill Agrícola S/A** e a **COOPCARGILL** segue as diretrizes da *Política Global de Uso da Tecnologia da Informação Corporativa.*

2.7.1 Abrangência

A Política de Risco Cibernética tem abrangência corporativa nas dependências da **COOPCARGILL**, ou seja, afeta todas as suas áreas de negócio, atendimento, administração e demais operações no que se refere à ocorrência de incidentes relativos ao risco cibernético de segurança da informação.

2.7.2 Objetivo

A **COOPCARGILL** estabelece as diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

- **i.** Proteger o valor e a reputação da empresa;
- **ii.** Garantir a confidencialidade, integridade e disponibilidade das informações da **COOPCARGILL** contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
- **iii.** Identificar violações de segurança cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

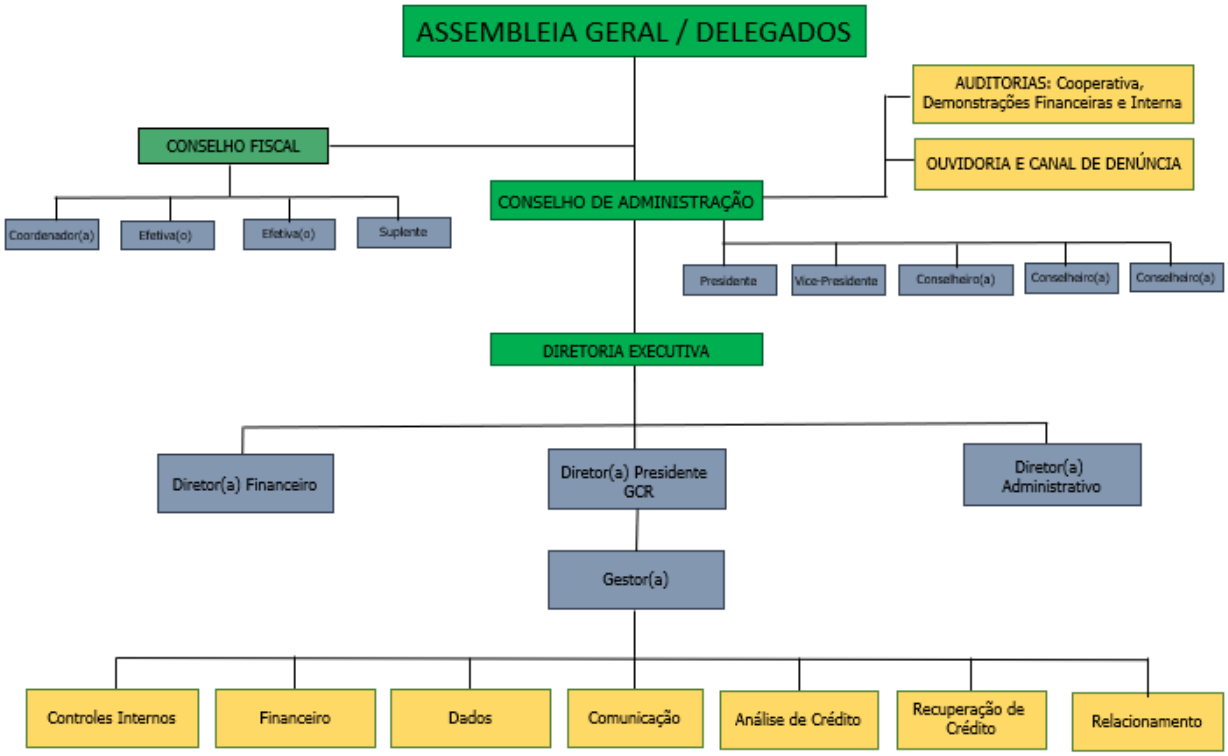
iv. Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

v. Atender aos requisitos legais, regulamentares e as obrigações contratuais pertinentes a atividade da empresa; e

vi. Conscientizar, educar e treinar os colaboradores por meio de política de Risco Cibernético, normas e procedimentos internos aplicáveis as suas atividades diárias;

vii. Estabelecer e melhorar continuamente o processo de gestão de riscos de segurança cibernética.

2.7.3 Organograma



2.7.4 Papéis e Responsabilidades.

2.7.4.1. Conselho de Administração

i. Definir diretrizes para implementação e aprovar a Política de Risco Cibernético;

ii. Acompanhar se as diretrizes definidas na Política estão sendo cumpridas;

iii. Acompanhar as alterações na legislação de forma a manter a Política sempre em conformidade com os normativos; e

iv. Garantir os recursos, inclusive tecnológicos, necessários para o desempenho das atividades da Instituição.

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

2.7.4.2. Diretoria Executiva

i. Desenvolver a Política que atenda ao porte e complexidade da **COOPCARGILL**;

ii. Implementar sistema de supervisão que demonstre que os controles de segurança da informação estão sendo devidamente executados e alinhados, conforme as exigências do Banco Central do Brasil;

iii. Prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação;

iv. Prover comprometimento e apoio à aderência a política de segurança cibernética e da informação de acordo com os objetivos e estratégias de negócios estabelecidas para a organização;

v. Prover e garantir a divulgação dessa política aos funcionários da **COOPCARGILL** e às empresas prestadoras de serviços terceirizados, mediante linguagem clara e acessível;

vi. Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da **COOPCARGILL**;

vii. Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso da **COOPCARGILL** incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;

viii. Analisar os riscos relacionados à segurança da informação da **COOPCARGILL** e propor a alçadas competentes, o aperfeiçoamento do ambiente de controle;

ix. Conduzir a gestão de incidentes de segurança da informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

x. Conduzir a definição de controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de segurança da informação;

xi. Designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;

xii. Autorizar acesso de seus colaboradores e terceiros apenas quando forem realmente necessários; e

xiii. Garantir a adoção de cláusulas pertinentes à segurança das informações nos contratos estabelecidos com a **COOPCARGILL**.

2.7.4.3. Colaboradores

i. Tomar conhecimento e seguir ao conteúdo desta Política e se comprometer a cumprir com o **Termo de Compromisso da Segurança da Informação – ANEXO I** para uso da rede e de ativos da informação (para funcionários, estagiários e prestadores de serviços);

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

ii. Utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de TI e assegurar que os recursos tecnológicos à sua disposição, sejam utilizados apenas para as finalidades aprovadas pela **COOPCARGILL**;

iii. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela **COOPCARGILL**;

iv. Garantir que as informações e dados de propriedade da **COOPCARGILL** não sejam disponibilizados a terceiros e nem discutidos em ambientes públicos ou em áreas expostas como avião, restaurantes, encontros sociais etc.;

v. Comunicar imediatamente qualquer fato ou ameaça à segurança dos recursos, tais como quebra da segurança, fragilidade, mau funcionamento, vírus, interceptação de mensagens eletrônicas, acesso indevido ou desnecessário a pastas/diretórios de rede, acesso indevido à Internet entre outros.

vi. Ter atenção quando do manuseio de informações confidenciais, a fim de evitar modificação, perdas ou divulgação não autorizada;

vii. Utilizar somente os recursos tecnológicos disponibilizados e permitidos pela Instituição;

viii. Não divulgar informações confidenciais; e

ix. Sanar toda e qualquer dúvida que possa surgir junto ao seu superior hierárquico.

Nota: Os colaboradores da **COOPCARGILL** passam pelo processo de integração na empresa mantenedora onde recebem um “notebook” como ferramenta de trabalho e os logins de acesso. Desta forma, a cooperativa está amparada pela Política Global da mantenedora. Os sistemas utilizados pela **COOPCARGILL** permitem o cadastramento de senhas individuais para cada colaborador ou membro estatutário, limitado à sua função. Assim, é permitido um melhor gerenciamento de entrada de informação, alteração e cancelamento de dados na base do sistema Syscoop 32 e Syscoop Web.

2.7.4.4. Conselho Fiscal

i. Acompanhar o plano de ação e de resposta a incidentes e verificar se o documento se encontra aprovado e se existem situações identificadas; e

ii. Checar eventuais fatos que ocasionaram paralizações de atividades.

2.7.4.5. Cooperados

i. Manter seus dados cadastrais junto a **COOPCARGILL** atualizados;

ii. Atualizar senha de acesso e não divulgar a outras pessoas; e

iii. Providenciar autorizações quando os procedimentos internos definidos pela **COOPCARGILL**, assim o exigirem.

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

2.7.4.6. Prestadores de Serviços

- **i.** Tomar conhecimento e seguir ao conteúdo desta Política e se comprometer conforme disposto nas cláusulas contratuais;
- **ii.** Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de hardware e software;
- **iii.** Informar imediatamente a Diretoria Executiva sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos da **COOPCARGILL**;
- **iv.** Sempre que solicitado, controlar e recomendar as alterações em ativos de TI e garantir que estes estejam em conformidade com suas licenças válidas;
- **v.** Preservar e garantir a continuidade dos serviços tecnológicos (rede) de forma a atender aos requisitos essenciais do negócio;
- **vi.** Cumprir as determinações da política, normas e procedimentos publicados pela **COOPCARGILL**;
- **vii.** Orientar os funcionários das empresas sobre o cumprimento das determinações da política, normas e procedimentos publicados pela **COOPCARGILL**;
- **viii.** Manter atualizado no Contrato de Serviços as cláusulas que versam sobre as obrigações e responsabilidades das partes;
- **ix.** Definir senhas para seus colaboradores quando do acesso ao sistema operacional da Instituição, autorizado previamente pela **COOPCARGILL**, com limitação de acesso;
- **x.** Fazer uso somente das informações que fazem parte especificamente do objeto de trabalho contratado;
- **xi.** Manter e assegurar os recursos tecnológicos necessários para garantir o desempenho das atividades executadas, sempre com segurança; e
- **xii.** Garantir que seus colaboradores executem suas atividades protegendo as Informações Confidenciais.

2.7.5 Implementação da Política Cibernética

A política é compatível com:

- **i.** o porte, o perfil de risco e o modelo de negócio da **COOPCARGILL**;
- **ii.** a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da **COOPCARGILL**; e
- **iii.** a sensibilidade dos dados e das informações sob responsabilidade da **COOPCARGILL**

2.7.6 Princípios de Segurança da Informação

Para os fins da divulgação e atendimento dessa política, consideram-se como partes interessadas: os colaboradores, os cooperados, os parceiros institucionais, os

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

fornecedores, os agentes reguladores e fiscalizadores, o governo, as associações de classe e a sociedade em geral, todos com foco no estímulo à prática de sustentabilidade social, ambiental e climática dos produtos e serviços.

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: controle de acesso e riscos cibernéticos. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

i. **Confidencialidade**: proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas, voluntária ou involuntariamente, dados restritos que deveriam ser acessíveis apenas por um determinado grupo de usuários.
ii. **Integridade**: garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.
iii. **Disponibilidade de Dados**: prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.
iv. **Acesso controlado**: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. A ameaça à segurança acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.
v. **Riscos Cibernéticos:** Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis; e
vi. **Autenticidade:** Esse processo realiza a tarefa de identificar e registrar o usuário que está enviando ou modificando a informação. Ou seja, autenticidade é quando um usuário vai manipular algum dado e ocorre uma documentação sobre essa ação. Todos esses métodos são importantes para garantir a segurança das informações corporativas das possíveis ameaças, que podem ter origens tanto externas quanto internas. Elas podem ser uma pessoa, um evento ou uma ideia capaz de causar danos ao sistema. As ameaças externas são tentativas de ataque ou desvio de informações vindas de fora da empresa, normalmente originadas por pessoas com

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

a intenção de prejudicar a corporação. As internas podem ser causadas por colaboradores de forma intencional. Essas ameaças podem causar pequenos incidentes e até prejuízos graves, por isso também devem ser levados em conta na hora do planejamento dos processos de segurança da empresa.

2.7.7 Controles da Segurança da Informação

A **COOPCARGILL** estabeleceu plano de ação e de resposta a incidentes aprovado pelo Conselho de Administração. São exigidos alguns controles básicos de segurança da informação:

- **i.** Política de Risco Cibernético e respectivo plano de ação que precisam ser aprovados pela Diretoria Executiva, *ad referendum* do Conselho de Administração;
- **ii.** Confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados;
- **iii.** Controles que considerem o porte da instituição, seu perfil de risco, seu modelo de negócio, seus produtos e a sensibilidade dos dados;
- **iv.** Controles e procedimentos com rastreabilidade para a garantia da proteção de informações sensíveis e classificação de dados ou de informações;
- **v.** Diretor responsável pela política de segurança cibernética, pela execução do plano de ação e pela gestão de incidentes;
- **vi.** Implementação de programas de capacitação em segurança;
- **vii.** Comunicação para clientes e usuários; e
- **viii.** Comprometimento da alta administração.

2.7.8 Registros de Incidentes Relevantes

Se refere ao registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da **COOPCARGILL** conforme **Anexo II - Relatório de Incidente de Segurança da Informação.**

O registro de incidentes toma uma importância muito grande nas normatizações relativas a esse assunto. É exigido a existência e formalização dos seguintes controles relacionados ao registro de incidentes:

- **i.** Descrição, Período em que ocorreu o incidente, Data/hora início/fim, Severidade do incidente, Tipo de Impacto, Origem do alerta, Comunicação do incidente, Detalhamento do Incidente, Tratamento do Incidente, Análise e Encerramento do Incidente;
- **ii.** Planos de ação e planos de resposta para incidentes;
- **iii.** Área específica para os registros de incidentes;
- **iv.** Plano de continuidade de negócio e relatório anual – Andamento do plano de ação e resposta para incidentes; e

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

v. Revisão anual pela Diretoria Executiva, *ad referendum* do Conselho de Administração.

Posteriormente, deverá ser observado o contido no comunicado **041/2022** de 14/11/2022 emitido pela **Federação Nacional das Cooperativas de Crédito - FNCC** em atendimento ao inciso VII, art. 3º da Resolução CMNº nº 4.893/2021, em que a **COOPCARGILL** poderá compartilhar as informações referentes as ocorrências de incidentes cibernéticos relevantes com as demais cooperativas por meio da **FNCC**, conforme instruções apresentadas naquele comunicado.

É importante ressaltar que o compartilhamento dessas informações por meio da **FNCC**, não desobriga a cooperativa de informar ao Banco Central do Brasil (BCB) os incidentes relevantes descritas no item **2.7.17. - Comunicações ao Banco Central do Brasil.**

São considerados como incidentes cibernéticos relevantes, de acordo com o comunicado, as interrupções de sistema não planejadas que podem ocorrer por ações diversas, que causam danos e afetem os negócios da cooperativa, como por exemplo:

i. queda de energia elétrica;
ii. falha de um elemento de conexão;
iii. servidor fora do ar, ausência de conexão com internet;
iv. sabotagem / terrorismo;
v. indisponibilidade de acesso a cooperativa; e
vi. ataques DDOS (um tipo de ataque cibernético, um invasor sobrecarrega um website, servidor ou recurso de rede com tráfego malicioso), entre outros.

2.7.9 Divulgação da Política de Risco Cibernético

A política de risco cibernético será divulgada aos funcionários da instituição e às empresas prestadoras de serviços através da página da **COOPCARGILL** na internet, no menu cooperado, quem somos – Política de Segurança Cibernética, podendo, a seu critério, considerar tais informações no contrato de prestação de serviço, quando necessário.

Os mecanismos para disseminação da cultura de segurança cibernética na **COOPCARGILL** são descritos a seguir:

i. a implementação de programas de capacitação e de avaliação periódica de pessoal;
ii. a prestação de informações aos associados e usuários sobre precauções na utilização de produtos e serviços financeiros; e
iii. o comprometimento da Diretoria Executiva com a melhoria contínua dos procedimentos relacionados com a segurança cibernética;

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

2.7.10 Plano de Ação e de Respostas à Incidentes

Fica estabelecido o plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética, que abrange:

- **i.** as ações a serem desenvolvidas pela **COOPCARGILL** para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;
- **ii.** as rotinas, os procedimentos, os controles e as tecnologias a serem utilizadas na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e
- **iii.** a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

Será elaborado relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, que deverá abordar, no mínimo:

- **i.** a efetividade da implementação das ações a serem desenvolvidas para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética
- **ii.** o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- **iii.** os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período (compartilhados, se houver, com a **FNCC** conforme descrito no item **2.7.8. Registros de Incidentes Relevantes**; e
- **iv.** os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionadas por incidentes.

O relatório será apresentado à Diretoria Executiva até 31 de março do ano seguinte ao da data-base que validará e levará para conhecimento do Conselho de Administração.

2.7.11 Avaliação e Contratação de Serviços de TI e de Processamento, Armazenamento de Dados e de Computação em Nuvem

A **COOPCARGILL**, tendo em vista o seu porte, o perfil de risco que se encontra exposta, bem como o modelo de negócio adotado e previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, adotará os seguintes procedimentos:

- **i.** Verificará se a empresa contratada adota práticas de governança corporativa e de gestão, proporcionais à relevância do serviço contratado e aos riscos a que estejam expostas; e
- **ii.** a verificação da capacidade do potencial prestador de serviço de assegurar:
  - **a.** o cumprimento da legislação e da regulamentação em vigor;

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

b. o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
c. a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
d. a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;
e. apresentação de relatório anual, até março de cada ano, com os testes realizados, investimentos, tratamento dos problemas ocorridos no período, backup etc., 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 **COOPCARGILL** por meio de controles físicos ou lógicos;
h. a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos cooperados da **COOPCARGILL;** e
i. Necessidade de acesso às informações/dados pelo Banco Central do Brasil.

A **COOPCARGILL** deve proceder a uma avaliação criteriosa quanto à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, considerando:

i. a criticidade dos serviços a serem prestados, e quando relevantes, aprovadas pela Diretoria Executiva depois de avaliação do potencial prestador de serviço candidato no atendimento à cooperativa, sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas pela empresa contratada;
ii. Verificação quanto a adoção, por parte do prestador de serviços de controles que mitiguem efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos no caso de serem executados através de internet;
iii. A **COOPCARGILL** deve possuir recursos e competências necessários para a adequada gestão dos serviços a serem contratados;
iv. A **COOPCARGILL** 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.

Conforme previsto na resolução CMN nº 4.893/2021, os serviços de computação em nuvem abrangem a disponibilidade à instituição contratante, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

i. Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais, que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

ii. Implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviço; e

iii. 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 **COOPCARGILL**, tendo em vista a necessidade de otimizar o atendimento de seus cooperados e visando maior segurança e celeridade, e baseado nas premissas citadas anteriormente, fez a contratação do Serviço de Computação em Nuvem.

O contrato foi firmado com a empresa PRODAF INFORMÁTICA que, é a responsável pelos serviços de processamento e armazenamento de dados conforme disposto na resolução CMN nº 4.893/21. Esta, por sua vez, possui contrato regular de Serviços junto a DEDALUS que, é detentora do espaço utilizado pela **COOPCARGILL** para armazenar seus dados.

Por sua vez, o espaço objeto do contrato entre a DEDALUS x PRODAF INFORMÁTICA pertence à AMAZON WEB SERVICES, conforme Termo de Adesão de Proposta Comercial 2850A.14, datado de 15/08/2014, onde foram escolhidas as seguintes opções de serviços: *Serviços de Hospedagem AWS – Franquia Mensal e Serviço de Suporte DEDALUS – Nível de Serviços Enterprise.*

O backup das máquinas da **COOPCARGILL** está em nuvem através da Microsoft - OneDrive, de forma que, permite o acesso às informações de qualquer lugar do mundo que contemple acesso à internet. As informações estão protegidas em nuvem.

2.7.12 Responsabilidade entre a COOPCARGILL e a mantenedora Grupo Cargill Agrícola S/A.

A **COOPCARGILL** poderá obter dados cadastrais de seus associados, em algumas situações específicas, tal como via importação cadastral (realizada mensalmente através do sistema nuvem Prodaf Informática e das empresas conveniadas) possibilitando atualização de dados cadastrais dos associados. Os dados fornecidos pelos associados e/ou empresas conveniadas serão mantidos em absoluto sigilo e, por esta razão, a **COOPCARGILL** assegura que eles não serão, sob nenhuma hipótese, vendidos, alugados, cedidos, nem de outra forma repassados a terceiros.

Além das disposições contidas neste documento, a **COOPCARGILL** afirma a sua conduta ética obrigando-se a cumprir, com rigor, as disposições legais vigentes no Brasil que tratam da privacidade, sigilo e segurança das informações que receber de seus associados e/ou das empresas conveniadas, com a finalidade maior de resguardar os direitos deles.

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

O principal objetivo dessa política é continuar demonstrando aos associados a forma ética aplicada pela **COOPCARGILL** em seus relacionamentos, sempre no intuito de buscar o melhor atendimento.

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função. Periodicamente, os acessos concedidos devem ser revistos pelo responsável da **COOPCARGILL**.

O identificador da rede e dos sistemas (login/senha) é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia. Seguem alguns cuidados que devem ser tomados:

- **i.** Manter a confidencialidade, memorizar e não registrar a senha em lugar algum, ou seja, não informar a ninguém e não a anotar em papel;
- **ii.** Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- **iii.** Selecionar senhas de qualidade, que sejam de difícil adivinhação;
- **iv.** Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- **v.** Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del).

2.7.13 Relatórios de testes de Segurança na Informação

A Prodaf realizará testes dos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente política, incluindo, mas não se limitando apenas aos procedimentos de descarte de informações pelos colaboradores, individualização dos usuários, dentre outros e estarão disponibilizados no site da Prodaf os relatórios periódicos.

Estes testes serão realizados pela equipe de suporte de TI da contratada, e buscará cobrir os seguintes pontos:

- **i.** Identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de hardware e software, além de processos que necessitem de proteção. Importante estimar impactos financeiros, operacionais e reputacionais em caso de evento;
- **ii.** Estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma a buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;
- **iii.** Detecção de possíveis anomalias e/ ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados; e

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

iv. Criação de plano de resposta e prevenção de incidentes que contenha comunicação interna e externa, se necessário. Serão realizados testes anuais para validar sua eficiência. O plano identificará papéis e responsabilidades, com previsão de acionamento de colaboradores e contatos externos.

Manter tal programa de segurança cibernética atualizado, identificando novos e potenciais riscos, ativos e processos.

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, deverão ser mantidas na **COOPCARGILL** como evidência em eventuais questionamentos internos ou de órgãos reguladores.

2.7.14 Continuidade dos Negócios

O processo de gestão de continuidade de negócios relativo à segurança da informação, é implementado para minimizar os impactos, e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através de: combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados em nuvem e os testes previstos para os cenários de ataques cibernéticos. Segue a adoção dos itens **2.8 Política de Continuidade de Negócios** e **2.8a. PCOL - Plano de Continuidade Operacional e de Liquidez.**

2.7.15 Reporte/Comunicação à Diretoria Executiva

Tendo em vista a complexidade que envolve o cumprimento da Política de Risco Cibernético, e a dificuldade da **COOPCARGILL** em validar ou não a efetivação dos procedimentos, é imperioso manter a Diretoria Executiva informada sobre indícios de irregularidades verificados quando do cumprimento das determinações dessa política.
Assim, caberá à PRODAF INFORMÁTICA realizar a comunicação de possíveis indícios quando de sua ocorrência ou, as verificações realizadas sob a ótica da gestão de acessos, proteção de ambientes, segurança física e lógica e continuidade do negócio.

2.7.16 Comunicações ao Banco Central do Brasil.

A **COOPCARGILL** informará previamente ao Banco Central do Brasil quando da contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, inclusive quando de alterações contratuais. Essa comunicação

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

deverá ser realizada até dez dias antes da contratação dos serviços e conter as seguintes informações, no mínimo:

i. Denominação da empresa a ser contratada;
ii. Os serviços relevantes a serem contratados; e
iii. A indicação de países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, nos casos de contratação no exterior.

Deverá haver comunicação tempestiva ao Banco Central do Brasil quando e se houver ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades. A comunicação será compartilhada, caso ocorram, com a **FNCC** conforme descrito no item **2.7.8. Registros de Incidentes Relevantes.**

2.7.17 Considerações Finais

A Política de Risco Cibernético será aprovada e revisada a cada 2 (dois) anos, pela Diretoria Executiva, ou quando houver exigências / alterações dos órgãos normativos, *ad referendum* do Conselho de Administração da **COOPCARGILL**. Além disso, deverá assegurar a divulgação deste documento, bem como manter toda a documentação relativa a este regulamento à disposição do Banco Central do Brasil.

Este documento é parte integrante da estrutura de controles internos e gerenciamento de riscos destacada no grupo: **1. Estrutura, item: 1.1 – ESTRUTURA DE CONTROLES INTERNOS**.

DocuSigned by: Alexandre Muniz 392683E83C484F4...	DocuSigned by: Edna Shinkawa FAC1DB2CA7CC42C...	DocuSigned by: HORACIO COSER FILHO FA2BE7C3874D4E0...
Alexandre Muniz da Silva Diretor Presidente	Edna Shinkawa Diretora Administrativa	Horácio Coser Filho Diretor Financeiro

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

2.7.18 ANEXO I - Termo de Compromisso da Política e Segurança da Informação.

O Funcionário/Prestador de Serviços abaixo qualificado declara ter conhecimento da Política Risco Cibernético e de sua responsabilidade no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este; em conformidade com esse termo firmado entre as partes.

DE ACORDO
E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CIÊNCIA é assinado pela parte declarante.

IDENTIFICAÇÃO DO CONTRATO (quando prestador de serviços)

N° / data do Contrato:	
Empresa Contratada:	
CNPJ:	
Objeto Resumido:	
Vigência Contratual:	

IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)

Nome:	Assinatura
CPF:	
Função	

Local, dia/mês/ano:

Docusign Envelope ID: 505F227E-DC35-4E4E-B3A0-D752026C269A

2.7.19 ANEXO II Relatório de Incidente de Segurança da Informação

Descrição	Identificar resumidamente sobre o incidente		
Período em que ocorreu o incidente			
Data/hora início: Data/hora fim:			
Severidade do incidente **(*)**	Alta ( )	Média ( )	Baixa ( )
Tipo de Impacto **(**)**	( ) Confidencialidade ( ) Integridade ( ) Disponibilidade		
Origem do alerta	Informar quem ou qual sistema alertou do incidente		
Comunicação do incidente	Informar a quem ou a quais setores o incidente foi informado.		
Detalhamento do Incidente	Descrição do ocorrido, o que foi impactado (ex. sistema), informações do prestador de serviço, o que foi afetado e demais informações importantes.		
Tratamento do Incidente	Descrever ações executadas para contenção e/ou contorno do problema/incidente, equipes/pessoas envolvidas, sistemas/ferramentas utilizadas para controle do incidente.		
Análise e Encerramento do Incidente	Descrever se necessárias outras ações e recursos necessários para finalizar o tratamento do incidente e/ou para evitar que o incidente volte a ocorrer.		