MANUAL DE CONTROLES INTERNOS

2.9. POLÍTICA DE SEGURANÇA E RISCO CIBERNÉTICO

SUMÁRIO

2. GERENCIAMENTO DE RISCOS.

2.9. Política de Risco Cibernético

2.9.1. Introdução

A **Cooperativa de Economia e Crédito Mútuo dos Servidores da Federação do Comércio, SESC, SENAC de São Paulo** como instituição financeira autorizada a funcionar pelo BACEN enquadrada no S5, segmento representado pelas instituições de menor porte e de perfil de risco simplificado, implementou estrutura simplificada de gerenciamento contínuo de riscos compatível com o modelo de negócio, com a natureza das operações e com a complexidade dos produtos, serviços, atividades e processos da instituição; proporcional à dimensão e à relevância da exposição aos riscos, segundo critérios definidos pela instituição e adequada ao perfil de riscos, uma vez que ela só atua com capital e empréstimos.

A política de segurança e risco cibernético tem como objetivo atender a resolução CMN – Conselho Monetário Nacional nº 4.893/21 e estabelecer os princípios, conceitos, valores e práticas, sobre os requisitos da contratação de serviços de processamentos e armazenamento de dados e de computação em nuvem que devem ser adotados pelos administradores e empregados da cooperativa.

A cooperativa incorpora em seus valores corporativos a convicção de que o exercício de suas atividades e a expansão de seus negócios devem se basear em princípios éticos, os quais devem ser compartilhados por todos os seus empregados. Na constante busca do seu desenvolvimento e da satisfação dos cooperados, a cooperativa busca transparência e cumprimento da legislação aplicável às atividades de administração e gestão de recursos de terceiros.

2.9.2. Responsabilidades

i. Diretoria Executiva

a) 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;

b) Prover todas as informações de gestão de segurança da informação definidas com o apoio de T.I e demais técnicos e consultores quando necessário;

c) Prover ampla divulgação da Política de Segurança da Informação, inclusive fornecendo treinamentos para todos os empregados da cooperativa;

ii. Diretor de Riscos

a) Criação, revisão e atualização da política de segurança e risco cibernético em conjunto com o gerente;

b) Analisar os riscos relacionados à segurança da informação da cooperativa e propor a alçadas competentes, o aperfeiçoamento do ambiente de controle.

iii. Gerente

a) Prover todas as informações de gestão de segurança da informação solicitadas pela Diretoria com o apoio de T.I e demais técnicos e consultores quando necessário;

b) Prover ampla divulgação da Política de Segurança da Informação, fornecendo treinamentos para todos os empregados da cooperativa;

c) Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da cooperativa;

d) Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso da cooperativa, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;

e) Analisar os riscos relacionados à segurança da informação da cooperativa e propor a alçadas competentes, o aperfeiçoamento do ambiente de controle.

iv. Dos Empregados em Geral

a) Cumprir essa política;

b) Tomar conhecimento 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 empregados, estagiários e prestadores de serviços);

c) Assegurar que os recursos tecnológicos à sua disposição, sejam utilizados apenas para as finalidades aprovadas pela cooperativa;

d) Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela cooperativa;

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

f) Comunicar imediatamente qualquer fato ou ameaça à segurança dos recursos, tais como quebra da segurança, fragilidade, mal funcionamento, vírus, intercepção de mensagens eletrônicas, acesso indevido ou desnecessário a pastas/diretórios de rede, acesso indevido à Internet entre outros;

g) Manter-se atualizado em relação a essa política e aos procedimentos e normas relacionadas, buscando orientação do coordenador sempre que não estiver completamente seguro quanto à aquisição, uso e/ou descarte de informações.

v. Técnicos de T.I. das empresas mantenedoras e prestadores de serviços de TI

a) Recomendar aquisição de equipamentos, aplicativos, antivírus e firewall para garantir a segurança e bom desempenho da Cooperativa;

b) Reportar a gerência as não conformidades com acessos físicos ou lógicos de empregados e prestadores de serviços;

c) Informar inconsistências ou erros em backup compartilhado de redes e pastas;

d) Informar mal funcionamento de nobreaks e demais equipamentos de segurança.

2.9.3. Meios Eletrônicos

Os meios eletrônicos utilizados pela cooperativa são:

- Correio eletrônico;
- Acesso à internet;
- Acesso físico;
- Acesso lógico em sistemas (operaciional, whatsapp corporativo, site, etc.);

Após a assinatura do termo de conhecimento da política de segurança e risco cibernético, a cooperativa poderá verificar e utilizar-se das informações para investigações futuras, leitura e/ou revisões que as áreas designadas fazem relativas às informações, dados, arquivos, conteúdo e mensagens que enviam, recebem, armazenam ou acessam.

Os acessos eletrônicos devem ser feitos para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas às empresas.

Os acessos físicos serão monitorados, caso seja necessário, a empresa apoiadora poderá fornecer a lista de acesso aos ambientes visitados.

A senha cadastrada é de uso pessoal e intransferível, não podendo ser cedida a terceiros.

2.9.4. Violações

A cooperativa se reserva ao direito de restringir ou cancelar o acesso a qualquer serviço, mensagens instantâneas, e-mail, mídia social ou página da internet, de forma total ou parcial.

Sites não relacionados ao negócio da instituição e/ou de conteúdo impróprio são expressamente proibidos. Em situações que sejam comprovados o uso de equipamentos de forma inadequada, os empregados e demais usuários serão notificados e poderão sofrer sanções determinados pela Diretoria Executiva.

A responsabilidade por esses acessos ou uso inadequado da informação é do usuário e poderá ser comprovada com relatório de acessos, login e senha.

2.9.5. Princípios da Segurança da Informação

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.

a) **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 voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários. A principal forma de mantê-la é por meio da autenticação, controlando e restringindo os acessos. Ela impõe limitações aos milhares de dados sigilosos que as empresas possuem. Sem a confidencialidade, as empresas ficam vulneráveis a ciber ataques, roubo de informações confidenciais e até utilização de dados pessoais de clientes, o que pode causar diversos prejuízos, inclusive financeiros.

b) **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.

c) **Disponibilidade**: 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.

d) **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.

e) **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 a intenção de prejudicar a corporação. As internas podem ser causadas por empregados 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.

f) **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.

2.9.6. Objetivos

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

a) Proteger o valor e a reputação da empresa;

b) Garantir a confidencialidade, integridade e disponibilidade das informações da cooperativa, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;

c) 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;

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

e) Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;

f) Conscientizar, educar e treinar os empregados por meio de política de Risco Cibernético, normas e procedimentos internos aplicáveis as suas atividades diárias;

g) Estabelecer e melhorar continuamente um processo de gestão de riscos de segurança cibernética.

2.9.7. Controles da Segurança da Informação

São exigidos alguns controles básicos de segurança da informação:

a) Política e plano de ação que precisam ser aprovados pela diretoria;

b) Confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados;

c) Controles que considerem o porte da instituição, seu perfil de risco, seu modelo de negócio, seus produtos e a sensibilidade dos dados;

d) Controles e procedimentos com rastreabilidade para a garantia da proteção de informações sensíveis e classificação de dados ou de informações;

e) Diretor responsável pela política de segurança cibernética, pela execução do plano de ação e pela gestão de incidentes;

f) Comunicação para clientes e usuários;

g) Comprometimento da alta administração.

2.9.8. Registros de Incidentes Relevantes

O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da cooperativa – **ANEXO II**. É exigido a existência e formalização dos seguintes controles relacionados ao registro de incidentes:

a) Identificação da causa e impactos dos incidentes;

b) Planos de ação e planos de resposta para incidentes;

c) Área específica para os registros de incidentes;

d) Plano de continuidade de negócio e relatório anual – Andamento do plano de ação e resposta para incidentes;

e) Revisão anual pela Diretoria Executiva;

f) A presente política tem que ser adotada por empresas prestadoras de serviços para a instituição, que manuseiem informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição.

2.9.9. Divulgação da Política de Segurança e Risco Cibernético

A política de segurança e risco cibernético será divulgada aos empregados da instituição 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.

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

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

b) A prestação de informações aos cooperados sobre precauções na utilização de produtos e serviços financeiros; e

c) O comprometimento da Diretoria Executiva com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

2.9.10. Plano de ação e de respostas a incidentes

Fica estabelecido plano de ação e de resposta a incidentes visando à implementação da política de segurança e risco cibernético que abrange:

I. As ações a serem desenvolvidas pela cooperativa para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança e risco cibernético;

II. As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança e risco cibernético; e

III. A área responsável pelo registro e controle dos efeitos de incidentes relevantes.

O relato sobre a ocorrência de segurança e risco cibernético, caso haja, constará no relatório anual de controles internos, que será apresentado a Diretoria Executiva entre 01 de janeiro e 30 de abril do exercício posterior.

A política de segurança e risco cibernético e o plano de ação e de resposta a incidentes mencionado devem ser aprovados pela Diretoria Executiva.

2.9.11. Avaliação e contratação de serviços de T.I., processamento, armazenamento de dados e computação em nuvem

A cooperativa previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, adotará os seguintes procedimentos:

I. 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

II. A 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, 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. O acesso da cooperativa aos relatórios elaborados por empresa de auditoria especializada independente, contratada pelo prestador de serviço;
   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 cooperativa por meio de controles físicos ou lógicos; e
   h. A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos cooperados da cooperativa.

A cooperativa deve avaliar a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem considerando:

   a. Criticidade dos serviços a ser 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;
   b. 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;

c. A cooperativa deve possuir recursos e competências necessários para a adequada gestão dos serviços a serem contratados;

d. A cooperativa 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.

Os serviços de computação em nuvem, se contratados, abrangem a disponibilidade à cooperativa, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

a. 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;

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

c. 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.

2.9.12. Comunicações ao Banco Central do Brasil

A cooperativa informará o 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 deverá ser realizada até dez dias após a contratação dos serviços e conter as informações:

I. Denominação da empresa contratada;

II. Os serviços relevantes a serem contratados;

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.

2.9.13. Responsabilidades da Cooperativa

A cooperativa poderá obter dados cadastrais de seus cooperados, em algumas situações específicas, tais como associação, atualização de dados, cadastro de endereço de e-mail, participação em promoções ou sorteios, consulta aos órgãos de proteção ao crédito.

Os dados fornecidos pelos cooperados serão mantidos em absoluto sigilo e, por esta razão, a cooperativa assegura que os mesmos não serão, sob nenhuma hipótese, vendidos, alugados, cedidos, nem de outra forma repassados a terceiros.

Além das disposições contidas neste documento, a Cooperativa 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 cooperados, com a finalidade maior de resguardar os direitos dos mesmos.

O principal objetivo dessa política é continuar demonstrando aos cooperados a forma ética aplicada pela cooperativa 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 gerente da cooperativa.

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:

a) Manter a confidencialidade, memorizar e não registrar a senha em lugar algum, ou seja, não fornecer a ninguém e não anotar em papel;

b) Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;

c) Selecionar senhas de qualidade, que sejam de difícil adivinhação;

d) Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;

e) Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del).

2.9.14. Aplicação

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

2.9.15. Serviços de Rede

A cooperativa utiliza os drivers da rede cedidos pelas empresas mantenedoras que são segmentadas para garantir a segurança e desempenho entre elas. Está implantado um sistema de prevenção de invasão na rede, e nos equipamentos para garantir a segurança da informação e disponibilidade de serviços.

2.9.16. Armazenamento de Dados

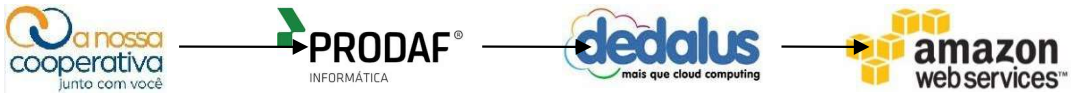
A cooperativa utiliza em parte a rede das empresas mantenedoras e as informações administrativas e de recursos humanos são armazenadas no servidor interno das empresas, que fica em um ambiente fechado (sala interna) com controle de acesso da equipe de T.I.

As informações operacionais, financeiras, contábeis, fiscais e indicadores são gerenciadas através do Sistema Operacional. Com isso seu armazenamento de dados (backup) é realizado de forma segregada a ser apresentada nos itens a seguir descritos.

2.9.16.1. PRODAF INFORMÁTICA LTDA.

A Prodaf, através do Syscoop32, realiza o gerenciamento sistêmico e o armazenamento de dados, onde há 11 módulos integrados que controla toda a parte operacional, financeira e contábil, da cooperativa.

A cooperativa optou por inserir as informações citadas em nuvem (cloud) através do contrato firmado com a Prodaf onde estão definidas as regras de segurança. Os contratos com a Prodaf envolvem as empresas subcontratadas Dedalus, que representa a empresa Amazon no Brasil, a qual é responsável pela guarda dos dados gerados pela cooperativa.



As principais qualidades que o sistema de gestão e a tecnologia Cloud, desenvolvidas pela Prodaf, agregam aos serviços oferecidos a praticidade, a agilidade e a segurança.

A cooperativa que está hospedada no cloud, nuvem da Prodaf, ambiente AWS – AMAZON, o nível de segurança ainda terá ferramentas de firewall, antivírus, ambos atualizados e monitorados diariamente, e análises constantes para detecção de possíveis ataques cibernéticos.

Com relação à política de back-up o ambiente cloud da Prodaf, tem Snaphots dos servidores, que são a imagem idêntica dos mesmos, armazenados 3 (três) por dia. Com essas imagens é possível restaurar o servidor com todas as configurações e discos

Além dos Snaphots, o sistema Prodaf disponibiliza para a cooperativa a ferramenta Bacula, onde há back-ups diários de arquivos, (back-up granular), das bases de dados da cooperativa, Banco Sybase, armazenados por 90 dias no S3/GLACIER (repositórios da AMAZON).

Os servidores são numerados e há um para cada serviço: internet, banco de dados, e-mail etc. Quando se conecta a um serviço, o computador acessa essa porta e usa um protocolo (essencialmente, um arquivo de texto descrevendo a comunicação entre as duas partes) para lidar com o servidor.

O conteúdo das nuvens é mediado para o usuário da cooperativa por meio da internet. O protocolo usado para acessar dados é o HTTP (o mesmo para acessar um site qualquer). Usando o protocolo e o domínio, se obtém exatamente na máquina com seus dados.

Para garantir a segurança, existe a barreira de login e senha e, servidores avançados, como o contratado pela cooperativa, também criptografam a comunicação com os cooperados. Além disso, toda informação enviada é particionada em vários pedaços para confundir um possível ataque hacker. Essa divisão não precisa ser necessariamente dentro do mesmo data center.

2.9.16.2. SESC

A empresa mantenedora Sesc, estende para a cooperativa a sua rede de informação (intranet, pacote office e e-mail), todos mediante acesso por senha de uso pessoal e intransferível.

Os servidores da empresa seguem o padrão de backup de e-mails corporativos, estendendo sua regra para os documentos da cooperativa, tendo sua tratativa idêntica às mensagens armazenadas para fins do negócio, tendo assim sua garantia de recuperação de informação, visto que os locais de armazenamento se encontram em ambiente fechado (sala interna) controlado com acesso restrito.

Quanto às informações guardadas de forma local, em computadores, a cooperativa orienta a seus empregados a utilizarem o drive específico, estabelecido na rede da empresa mantenedora, assegurando assim o backup automatizado.

2.9.17. Relatório de Testes de Segurança das Informações

Sempre que solicitado pela cooperativa, o departamento de TI da 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 empregados, individualização dos usuários, dentre outros.

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

a) 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;

b) Estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;

c) Detecção de possíveis anomalias e/ ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;

d) Criação de um plano de resposta e recuperação de incidentes, que contenha comunicação interna e externa, se necessário e terá testes anuais para validar sua eficiência. O plano identificará papéis e responsabilidades, com previsão de acionamento de empregados e contatos externos;

e) 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 cooperativa como evidência em eventuais questionamentos internos ou de órgãos reguladores ou autorreguladores.

2.9.18. Continuidade dos Negócios

O processo de gestão de continuidade de negócios relativo a 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 da combinação de requisitos como operações, empregados 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 de nuvem e os testes previstos para os cenários de ataques cibernéticos.

Com base nos procedimentos executados pelas empresas mantenedoras e PRODAF, considerando os controles de rede, internet e acessos, a cooperativa realizará o registro, análise da causa e do impacto e interrupção dos serviços relevantes, promovendo assim a transparência de suas informações, antecipando incidentes ou manutenção preventiva que possa impactar o seu devido funcionamento.

As informações de reinício ou normalização das suas atividades serão informadas tempestivamente aos cooperados em todos os canais de comunicação disponíveis.

A Diretoria Executiva da cooperativa informará ao Banco Central do Brasil as ocorrências de incidentes relevantes, considerando as interrupções, situações de crise e providências para a readequação e retorno de suas atividades.

2.9.19. Considerações Finais

A Política de Risco Cibernético será aprovada e revisada, periodicamente, pela Diretoria Executiva da cooperativa.

A cooperativa deverá: designar diretor responsável pelo cumprimento da Política de Risco Cibernético, formalizar e assegurar sua divulgação interna e externa; manter documentação relativa à disposição do Banco Central do Brasil.

Este documento é parte integrante da estrutura de controles internos e gerenciamento de riscos. Conheça a estrutura completa no **ANEXO I - ESTRUTURA DE CONTROLES INTERNOS E GERENCIAMENTO DE RISCOS** destacada no grupo 1.Estrutura, item: **1.1 - ESTRUTURA DE CONTROLES INTERNOS**.

jackson.matos@sescsp.org.br
Assinado
D4Sign
Jackson Andrade de Matos
Diretor Presidente

jprimolan@sp.senac.br
Assinado
D4Sign
José Claudinei Primolan
Diretor Administrativo

ntakarabe@fecomercio.com.br
Assinado
Noboru Takarabe
D4Sign
Noboru Takarabe
Diretor Financeiro

jhenrique@sp.senac.br
Assinado
João Henrique de Freitas Alves
D4Sign
João Henrique de Freitas Alves
Diretor de Operações

raquel.claro@sescsp.org.br
Assinado
Raquel Claro Vargas
D4Sign
Raquel Claro Vargas
Diretora de Planejamento

ricardo.gentil@sescsp.org.br
Assinado
Ricardo Gentil
D4Sign
Ricardo Gentil de Oliveira
Diretor de Comunicação

ANEXO I - TERMO DE COMPROMISSO E CONFIDENCIALIDADE

POLÍTICA DE SEGURANÇA E RISCO CIBERNÉTICO

O abaixo qualificado declara ter conhecimento da política de segurança e risco cibernético e de suas responsabilidades 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 da cooperativa ou nas dependências da empresa mantenedora SESC.

Considerando a natureza da atividade da cooperativa e as informações disponibilizadas em várias formas, podendo estar impressa, escrita, guardada ou transmitida por meios eletrônicos, correio, mostrada em filmes ou em conversações, comprometo-me a cumprir o sigilo, guarda e acesso somente ao que for necessário para o desempenho de minha função conforme contrato de trabalho / prestação de serviço.

Tratarei as informações com sigilo e ética, garantindo sob as penas da lei o fiel cumprimento da política de segurança e risco cibernético.

Confirmo que a segurança da informação é um ativo crítico para os negócios da cooperativa e deve estar protegida e utilizada somente para os fins específicos ao qual fui designado atendendo as definições:

a) DISPONIBILIDADE: é a garantia que aqueles autorizados tenham acesso à informação sempre que necessário;
b) INTEGRIDADE: é a garantia que a informação não sofreu modificação não autorizadas;
c) CONFIDENCIALIDADE: é a garantia que a informação é acessada somente por aqueles autorizados.

E por ser de livre manifestação de vontade, firmo o presente em duas vias

São Paulo, xx de xxxxx de 2024

Assinatura: _____

Nome:

CPF:

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.		

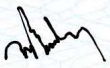
2 9 Política de Segurança e Risco Cibernético pdf

Código do documento cdcb86e7-5266-419f-98b5-637445ab330c

Assinaturas

Jackson Andrade de Matos
jackson.matos@sescsp.org.br
Assinou

José Claudinei Primolan
jprimolan@sp.senac.br
Assinou



Noboru Takarabe
ntakarabe@fecomercio.com.br
Assinou

Noboru Takarabe

João Henrique de Freitas Alves
jhenrique@sp.senac.br
Assinou

João Henrique de Freitas Alves

Raquel Claro Vargas
raquel.claro@sescsp.org.br
Assinou

Raquel Claro Vargas

Ricardo Gentil
ricardo.gentil@sescsp.org.br
Assinou

Ricardo Gentil

Eventos do documento

29 Feb 2024, 18:44:46
Documento cdcb86e7-5266-419f-98b5-637445ab330c **criado** por FABIANA FRANCISCHINI (798ab0e9-d6b3-468a-aa32-46e5c846a83b). Email:cooperativa@sescsp.org.br. - DATE_ATOM: 2024-02-29T18:44:46-03:00

29 Feb 2024, 18:47:05
Assinaturas **iniciadas** por FABIANA FRANCISCHINI (798ab0e9-d6b3-468a-aa32-46e5c846a83b). Email: cooperativa@sescsp.org.br. - DATE_ATOM: 2024-02-29T18:47:05-03:00

29 Feb 2024, 18:49:50
NOBORU TAKARABE **Assinou** (915b3be0-6437-4317-b9ec-2122c3113eef) - Email: ntakarabe@fecomercio.com.br - IP: 187.89.73.3 (ip-187-89-73-3.user.vivozap.com.br porta: 24164) - Geolocalização: -23.5983184 -46.641581 - Documento de identificação informado: 682.964.108-00 - DATE_ATOM: 2024-02-29T18:49:50-03:00

01 Mar 2024, 12:55:26

RAQUEL CLARO VARGAS **Assinou** - Email: raquel.claro@sescsp.org.br - IP: 187.50.135.90 (187.50.135.90 porta: 39010) - Geolocalização: -23.5454 -46.5839 - Documento de identificação informado: 256.107.368-89 - DATE_ATOM: 2024-03-01T12:55:26-03:00

01 Mar 2024, 16:10:16
RICARDO GENTIL **Assinou** - Email: ricardo.gentil@sescsp.org.br - IP: 187.50.135.90 (187.50.135.90 porta: 43716) - Documento de identificação informado: 163.629.678-52 - DATE_ATOM: 2024-03-01T16:10:16-03:00

01 Mar 2024, 16:33:16
JOÃO HENRIQUE DE FREITAS ALVES **Assinou** (e2ec93a4-0e5e-442d-8db2-b304f0d98402) - Email: jhenrique@sp.senac.br - IP: 186.239.253.60 (186.239.253.60 porta: 38496) - Geolocalização: -23.545971 -46.65073 - Documento de identificação informado: 144.324.798-76 - DATE_ATOM: 2024-03-01T16:33:16-03:00

05 Mar 2024, 09:31:49
JACKSON ANDRADE DE MATOS **Assinou** - Email: jackson.matos@sescsp.org.br - IP: 187.50.135.90 (187.50.135.90 porta: 33344) - Documento de identificação informado: 151.438.948-75 - DATE_ATOM: 2024-03-05T09:31:49-03:00

11 Mar 2024, 10:21:50
JOSÉ CLAUDINEI PRIMOLAN **Assinou** (4c540f70-3bcb-44f1-84d0-995fe71c94c8) - Email: jprimolan@sp.senac.br - IP: 179.94.34.41 (179-94-34-41.user.vivozap.com.br porta: 19938) - Documento de identificação informado: 080.399.498-23 - DATE_ATOM: 2024-03-11T10:21:50-03:00

Hash do documento original
(SHA256):f0cb42d31a37127da8f4da5e19a76fc7aecb2ade829d028db7ea8705ab821b45
(SHA512):25552be10d1d00799637091a22ca0c1b6b396ebac693bbe88bd038793ed05f6e9ea1be1eba072b07d400c48bb800bb6d163290cfe21bc5168ebb14dec29e0cdc

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign