Cretovale

somos coop

COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS TRABALHADORES DA VALE

POLÍTICA SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO 2024

RESOLUÇÃO DO CMN Nº 4.893/21

Cretovale
somos coop
COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS TRABALHADORES DA VALE

ÍNDICE

1. INTRODUÇÃO

A Política de Segurança Cibernética e da Informação é o documento que estabelece conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança cibernética e segurança da informação, visando preservar a confidencialidade, integridade, disponibilidade e conformidade de todas as informações sob gestão da CRETOVALE. Definir os princípios fundamentais que formam a base da Política de Segurança Cibernética e da Informação, norteando a elaboração de normas, processos, padrões e procedimentos.

A presente política tem abrangência corporativa nas dependências da CRETOVALE, ou seja, afeta todas as suas áreas de negócio, atendimento, administração e demais operações no que se refere a ocorrência de incidentes relativos ao risco cibernético de segurança da informação.

2. CONCEITO E DEFINIÇÕES

Para melhor compreensão da necessidade de se cumprir o descrito na Política deSegurança Cibernética e da Informação, é necessário conhecer os conceitos que fazem parte desse segmento, onde a informação é extremamente valiosa e passível de riscos que colocam em xeque a continuidade da cooperativa. Dessa forma, temos os seguintes conceitos para facilitar o entendimento:

Recursos: qualquer ativo, tangível ou intangível, pertencentes, a serviço ou sob responsabilidade da cooperativa, que possua valor para a mesma. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.

Ameaça: qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais.

Controle: qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controles materializa a segurança das informações. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware e outros.

Informação: qualquer conjunto organizado de dados que possua algum propósito e valor para a cooperativa, seus associados, parceiros e

colaboradores. A informação pode ser de propriedade da cooperativa, estar sob sua custódia ou sob custódia de terceiros, como por exemplo, informações armazenadas em nuvem.

Risco: qualquer evento que possa afetar a capacidade da companhia de atingir seus objetivos e sua estratégia de negócios ou o efeito da incerteza nos objetivos.

Política de Segurança Cibernética e da Informação: estrutura de documentos formada pela política, normas e padrões de segurança cibernética e segurança da informação.

Segurança da Informação (SI): é a proteção das informações, sendo caracterizada pela preservação de:

I. **Confidencialidade**: garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;
II. **Integridade**: garantia de que o conteúdo da mensagem não será alterado ou violado indevidamente, ou seja, mede a exatidão da informação e seus métodos de modificação, manutenção e validade.
III. **Disponibilidade**: garantia de que os colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessários, nos períodos e ambientes aprovados pela cooperativa;
IV. **Conformidade**: garantia de que controles de segurança da informação, devidamente estabelecidos, estão sendo executados conforme esperado e produzindo resultados efetivos no cumprimento de seus objetivos.

Segurança Cibernética: conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Também conhecida como **Segurança de TI**, visa proteger somente assuntos relacionados ao digital.

Nuvem (Cloud): infraestrutura, plataforma, aplicação ou serviço localizado na internet. A nuvem pode ser pública com acesso a todos, privada, com acesso restrito ou híbrido, com parte restrita e parte irrestrita.

3. PAPÉIS E RESPONSABILIDADES

A Cooperativa, através da sua Diretoria em conjunto com demais colaboradores cria a Política de Segurança Cibernética e da Informação, bem como os requisitos para a contratação, avaliação e gestão de serviços de processamento e armazenamentode dados e de computação em nuvem

visando total observância e adequação ao exigido na Resolução CMN 4.893/21.

A alta gestão tem o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

Essa política se aplica a todos os colaboradores, fornecedores e prestadores de serviços que utilizem ou forneçam serviços tecnológicos relevantes.

Diretoria:

i. Definir diretrizes para implementação e aprovar a Política de Segurança Cibernética e da Informação;
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;
iv. Garantir os recursos, inclusive tecnológicos, necessários para o desempenho das atividades da cooperativa;
v. 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;
vi. Prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação;
vii. 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 cooperativa;
viii. Prover e garantir a divulgação dessa política aos funcionários da cooperativa e às empresas prestadoras de serviços terceirizados, mediante linguagem clara, acessível, inclusive fornecendo treinamentos em nível de detalhamento compatível com as funções desempenhadas e sensibilidade das informações;
ix. Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação na cooperativa;
x. 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;
xi. Analisar os riscos relacionados à segurança da informação da cooperativa e propor a alçadas competentes, o aperfeiçoamento do ambiente de controle;
xii. Conduzir a gestão de incidentes de segurança da informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

xiii. Conduzir a definição de controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de segurança da informação;
xiv. Designar um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;
xv. Autorizar acesso de seus colaboradores e terceiros apenas quando forem realmente necessários;
xvi. Garantir a adoção de cláusulas pertinentes à segurança das informações nos contratos estabelecidos com a cooperativa.

Colaboradores:

i. Tomar conhecimento e seguir ao conteúdo desta Política e se comprometer a cumprir com o **TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO – ANEXO I** para uso da rede e de ativos da informação (para funcionários, estagiários e prestadores de serviços);
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 cooperativa;
iii. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela cooperativa;
iv. 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 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, intercepção de mensagens eletrônicas, acesso indevido ou desnecessário a pastas/diretórios de rede, acesso indevido à Internet entre outros.
vi. Modificação, perdas ou divulgação não autorizada;
vii. Utilizar somente os recursos tecnológicos disponibilizados e permitidos pela cooperativa;
viii. Não divulgar informações confidenciais;
ix. Sanar toda e qualquer dúvida que possa surgir junto ao seu superior hierárquico.

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;

ii. Checar eventuais fatos que ocasionaram paralizações de atividades.

Associados:

i. Manter seus dados cadastrais junto a cooperativa atualizados;
ii. Atualizar senha de acesso e não divulgar a outras pessoas; e
iii. Providenciar autorizações quando os procedimentos internos definidos pela cooperativa, assim o exigirem.

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 sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos da cooperativa;
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 cooperativa;
vii. Orientar os funcionários das empresas sobre o cumprimento das determinações da política, normas e procedimentos publicados pela cooperativa;
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 cooperativa, autorizado previamente pela cooperativa, 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.

4. DIRETRIZES GERAIS

A informação é um ativo essencial para os negócios da cooperativa, e através da segurança cibernética e da informação, compete proteger as informações contra diversos tipos de ameaças, para minimizar a exposição da cooperativa a riscos, garantindo que as características fundamentais da informação sejam preservadas, sendo elas: confidencialidade, integridade, disponibilidade e conformidade.

Alinhado com os objetivos e requisitos do negócio, a Política estabelece regras e direcionamentos a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações da cooperativa, de seus associados, fornecedores e parceiros de negócios.

Seguir as diretrizes desta política, significa proteger a cooperativa contra o vazamento de informações, contra fraudes, zelar pela privacidade, garantir que sistemas e informações estejam disponíveis quando necessário e zelar pela proteção da imagem e da marca da cooperativa.

Adoção de Comportamento Seguro:

Independentemente do meio e/ou da forma em que se encontrem, as Informações Sigilosas podem ser encontradas na sede da CRETOVALE e fazem parte do ambiente de trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção delas que os Colaboradores adotem comportamento seguro e consistente.

Na CRETOVALE, o processo relacionado à cultura de segurança cibernética compreende os seguintes procedimentos:

a) Programa de conscientização realizado anualmente;
b) A Diretoria da CRETOVALE é responsável por implementar e manter o programa de conscientização;
c) Novos colaboradores devem ser treinados sobre a Política de Segurança Cibernética e da Informação;
d) Associados da CRETOVALE são informados sobre precaução no uso de seus serviços através dos canais de comunicação e atendimento utilizados pela cooperativa;
e) A Diretoria da CRETOVALE é responsável por compartilhar alterações nos procedimentos de segurança da informação da CRETOVALE através de e-mail para colaboradores e através do site da cooperativa para os associados.

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela CRETOVALE. Desde que não haja abusos, o eventual uso do e-mail para assuntos particulares é tolerado. É terminantemente proibido o envio de mensagens e arquivos anexos que

possam causar constrangimento a terceiros, bem como conteúdo político ou outro que possa colocar a CRETOVALE em risco.

A CRETOVALE se reserva o direito de monitorar o uso dos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus Colaboradores, e que os registros e o conteúdo dos arquivos assim obtidos poderão ser utilizados para detecção de violações aos documentos internos da cooperativa e conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

A Diretoria da CRETOVALE implantará as medidas necessárias para realizar o monitoramento, bem como para estabelecer as permissões de acesso aos documentos e arquivos da CRETOVALE. Nesse sentido, o monitoramento poderá ser realizado por CONTRATADA mediante:

a) Gravação em vídeo do ambiente da cooperativa;
b) Registro de mensagens de e-mail;
c) Registro de acesso à Internet;
d) Registro de acesso à rede interna;
e) Registro de acesso a documentos e arquivos.

Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pela CONTRATADA.

Apenas a CONTRATADA poderá acessar os arquivos contendo as gravações e registros do monitoramento realizado, bem como, mediante autorização prévia da Diretoria da CRETOVALE poderá contratar prestadores de serviços externos para realizar o monitoramento.

O acesso será realizado aleatoriamente, de maneira inopinada e sem periodicidade definida. Os documentos, dados e informações encaminhadas pelos prestadores de serviços serão para uso exclusivo da Diretoria da CRETOVALE.

Sempre que necessário será lavrado termo de monitoramento e acesso aos arquivos contendo registros e gravações.

Gestão de Acesso a Sistemas de Informação e a Outros Ambientes Lógicos:

O uso das Informações Sigilosas e dos recursos de tecnologia disponibilizados pela CRETOVALE é monitorado, e os registros decorrentes do uso poderão ser utilizados para verificação e evidência da adequação das regras desta Política, e demais regras internas da cooperativa, através de monitoramento a ser efetuado pela CONTRATADA.

Todo acesso às Informações Sigilosas, aos ambientes lógicos e à sede da CRETOVALE deve ser controlado, de forma a garantir permissão apenas às pessoas expressamente autorizadas pela Diretoria da CRETOVALE.

O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

a) Pedido formal de concessão e cancelamento de autorização de acesso do usuário aos sistemas;
b) Utilização de identificador do Colaborador (ID de Colaborador) individualizado, de forma a assegurar a responsabilidade de cada Colaborador por suas ações e omissões;
c) Verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador e se é consistente com a Política de Segregação das Atividades;
d) Remoção imediata de autorizações dadas aos Colaboradores afastados ou desligados da CRETOVALE, ou que tenham mudado de função, se for o caso; e
e) Revisão periódica das autorizações concedidas.

Utilização da Internet:

O uso da Internet deve restringir-se às atividades relacionadas aos negócios e serviços da CRETOVALE, e para a obtenção de informações e dados necessários ao desempenho dos trabalhos.

Sites na Internet

O acesso a sites externos na Internet é monitorado. Os arquivos contendo os registros das tentativas de acesso e dos acessos são armazenados nos servidores da CONTRATADA.

Adicionalmente, o Diretor Responsável pela Política de Segurança Cibernética e da Informação no UNICAD poderá ser informado sobre acessos e tentativas de acesso a determinados sites.

Ramais Telefônicos:

O ramal telefônico utilizado pela OUVIDORIA da CRETOVALE é gravado, e o conteúdo das conversas é armazenado em arquivos no servidor da CONTRATADA. Conforme já esclarecido anteriormente, a Diretoria da CRETOVALE possui livre acesso às gravações com o propósito de verificação de conteúdo.

Telefones Celulares:

Os Colaboradores deverão evitar utilizar telefones celulares durante o horário de expediente enquanto estiverem na sede da CRETOVALE. Os aparelhos deverão ser mantidos no modo “silencioso” e somente poderão ser atendidas ligações pessoais de reconhecida importância para a cooperativa.

Mensagens Instantâneas:

A comunicação por mensagens instantâneas de texto e voz pela Internet para assuntos particulares deve ser evitada durante o horário de expediente, enquanto os Colaboradores estiverem na sede da CRETOVALE, mas não está proibida. Em caso de necessidade, os Colaboradores devem permitir o acesso a todas as mensagens instantâneas com o propósito de avaliar eventuais infrações ao disposto nos documentos internos.

Utilização e Conexão de Equipamentos:

Somente é permitido o uso de equipamentos homologados e devidamente contratados pela CRETOVALE.

A utilização de equipamentos pessoais por terceiros nas instalações da CRETOVALE e a conexão destes na rede interna e à Internet requer autorização prévia e expressa a Diretoria da CRETOVALE. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.

A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) somente poderá ser realizada mediante autorização prévia e expressa da Diretoria da CRETOVALE.

Acesso de Terceiros:

O acesso de terceiros aos arquivos e sistemas da CRETOVALE será possível, na forma definida pelo o Diretor Responsável pela Política de Segurança Cibernética e da Informação no UNICAD, mas deve sempre ser precedido da assinatura de um contrato de confidencialidade que estabeleça penalidade no caso de infração. Ademais, o terceiro deverá garantir à cooperativa, ainda que contratualmente, de que possui os controles necessários à boa guarda e proteção das informações aos quais terá acesso.

05 - CONCEITOS PARA CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da Informação tem o objetivo de proporcionar ao usuário a possibilidade de analisar suas informações, facilitando a definição do seu nível de acesso e condições de armazenamento, considerando sua confidencialidade, integridade e disponibilidade.

Todas as informações devem ser classificadas e deverá ser considerada sigilosa e de alto risco até que se tenha estabelecido sua classificação.
A proteção proporcionada à informação, tanto em termos de acesso quanto de conservação, deve estar de acordo com sua classificação.

Conceitos de Confidencialidade, os tipos de informações podem ser:

I. **Informações Sigilosas**: Informações extremamente restritas quanto a sua divulgação. São de alto valor por motivos estratégicos e/ou com grande possibilidade de provocar prejuízos, razão pela qual seu nível de proteção deve ser o mais alto possível;
II. **Informações Confidenciais**: Informações de caráter setorial e para divulgação a um reduzido grupo de pessoas de uma área ou setor de atividade;
III. **Informações Internas**: São aquelas que têm sua circulação restrita ao âmbito interno da cooperativa divulgadas a colaboradores e associados;
IV. **Informações Públicas**: São aquelas que circulam livremente, interna e externamente, em relação a cooperativa não havendo interesse em controlar sua divulgação e acesso.

Conceitos de Restrição ao Acesso, as restrições ao acesso podem ser:

I. **Controlado**: O acesso às informações sigilosas, confidenciais e internas, deverá ser determinado pela Diretoria, que estabelecerá as áreas, pessoas e o nível desse acesso;
II. **Não controlado**: As informações públicas não estarão sujeitas ao controle de acesso.

Conceitos de Níveis de Acesso, os níveis de acesso podem ser:

I. **Somente para consulta**: Nível de acesso do usuário permite somente a leitura das informações.
II. **Consulta e alteração**: Nível de acesso do usuário permite efetuar mudanças nas informações disponibilizadas, como inclusão de pareceres, informações complementares, valores, etc.

Conceitos de Integridade e Disponibilidade, a integridade e disponibilidade podem ser:

I. **De Alto Risco**: Informações cuja indisponibilidade e/ou inexatidão poderão causar prejuízos à continuidade dos negócios.
II. **De Médio Risco**: Informações que impõem ao negócio problemas de disponibilidade e dificuldade na recuperação. O proprietário da informação e os usuários aceitam a disponibilidade limitada e a existência de um determinado tempo para recuperação.
III. **De Baixo Risco**: Informações cuja exatidão e acessibilidade apresentam pouco ou nenhum risco ao negócio. Os usuários aceitam eventuais indisponibilidades e longos períodos para recuperação das informações.

06 - PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, a cooperativa adota os seguintes processos.

Gestão de Ativos da Informação:

- Entende-se por Ativos da Informação todos os tipos de dados que se pode criar, processar, armazenar, transmitir, alterar e excluir. Podem ser tecnológicos (“software” e “hardware”) e não tecnológicos (pessoas, processos e dependências físicas).
- Os ativos da informação devem ser identificados de forma individual, inventariado e protegido de acesso indevido, fisicamente e logicamente, ter documentos e planos de manutenção.

Classificação da Informação:

- As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Sigilosas, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

Gestão de Acessos:

- As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da cooperativa.

- Os acessos devem ser rastreáveis, a fim de garantir que ações são passiveis de auditoria possam identificar individualmente o Colaborador, para que seja responsabilizado por suas ações.

Gestão de Riscos:

- Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidade, ameaças e impactos sobre os ativos de informação da cooperativa, para que sejam recomendadas as proteções adequadas.
- Os cenários de riscos de segurança da informação são escalonados nos setores apropriados, para decisão.

Mitigação dos Riscos:

- A Cooperativa oferece aos Colaboradores estrutura tecnológica para o exercício das atividades, sendo responsabilidade de cada Colaborador manter e zelar pela integridade dessas ferramentas de trabalho, e por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade (computador, notebook, acesso à internet, e-mail, etc.).
- Equipamentos e computadores disponibilizados aos Colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da cooperativa.
- A instalação de copias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores da cooperativa depende de autorização do Diretor responsável pela Política devendo observar os direitos de propriedade intelectual pertinentes, tais como copyright, licenças e patentes.
- As mensagens enviadas ou recebidas através de correio eletrônico corporativo (e-mails corporativos), seus respectivos anexos, e a navegação através da rede mundial de computadores (internet) através de equipamentos da cooperativa poderão ser monitoradas.
- As senhas de acesso aos dados contidos em todos os computadores, bem como nos e-mails, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros.
- O colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.
- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), não devem ser baseadas em

informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome de empresa, nome de departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcde”, “12345”, entre outras.

- Os usuários podem alterar a própria senha e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Tratamento de Incidentes de Segurança da Informação:

Incidentes são interrupções de sistema não planejadas que ocorrem de várias naturezas e que afetam os negócios da cooperativa, como por exemplo:

- Queda de energia elétrica;
- Falha de um elemento de conexão;
- Servidor fora do ar;
- Ausência de conexão com internet;
- Sabotagem/terrorismo;
- Indisponibilidade de acesso a cooperativa;
- Ataques DDOS.

Qualquer colaborador que detectar um incidente deverá comunicar imediatamente ao Diretor Responsável pela Política.

Segurança Física do Ambiente:

O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas.

Controle de Prestadores de Serviços que manuseiam dados ou informações sensíveis:

Os prestadores de serviços que detenham informações sensíveis ou que sejam relevantes para condução das atividades operacionais da cooperativa, deverão ser tecnicamente capacitados e extremamente envolvidos com as atividades da cooperativa, de forma íntegra e responsabilizados sobre qualquer dano ou vazamento de informações de acordo com contrato de prestação de serviço e políticas internas da cooperativa. O acesso a qualquer informação deverá ser solicitado formalmente por e-mail, ao Responsável na Cooperativa.

07- GERENCIAMENTO DE INCIDENTES

Tem o objetivo de assegurar que os eventos de segurança de informação sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo sobre os sistemas de informação da cooperativa.

Avaliação Inicial:

Avaliar o incidente em conjunto com a ou Diretoria para verificar se é provável a sua reincidência ou se é um sintoma de problema crônico, para a tomada de providências e medidas corretivas.
Analisar motivos e consequências imediatas, bem como a gravidade da situação.

Incidente Caracterizado:

Caracteriza o incidente, devem ser tomadas as medidas imediatas, tais como:

- O Diretor responsável pela política estará avaliando o impacto do incidente nos diversos riscos envolvidos;
- Conforme a relevância (sabotagem, terrorismo, etc) poderá ser registrado um boletim de ocorrência ou queixa crime para as devidas providencias;
- Conforme a relevância do incidente comunicar os cooperados que por ventura foram afetados;
- Comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções de serviços relevantes, que configurem uma situação de crise pela cooperativa.

Recuperação:

Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência acionada e terceiros notificados.
Quaisquer dados que estejam faltando ou que estejam corrompidos, ou problemas identificados por colaboradores internos devem ser comunicados a Diretoria.

Retomada:

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar a operação normal, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção.

Relatório sobre implementação do Plano de Ação e de Resposta a Incidentes:

Será parte integrante do relatório de controles internos e do relatório integrado de gestão de risco da cooperativa, tendo em vista a complexidade e ao porte da mesma, e deve contemplar, no mínimo, as seguintes informações:

- A efetividade da implementação das ações relativas à implementação da Política de Segurança Cibernética e da Informação;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- Os resultados de testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

Deverá ser elaborado até 31 de março do ano seguinte ao da data base e aprovado pela Diretoria em ata de reunião.

08 - EXIGÊNCIAS PARA CONTRATAÇÃO DE SERVIÇOS EM NUVEM

A Cooperativa ao realizar contratações de serviços relevantes e armazenamento de dados e de computação em nuvem, no país ou no exterior deverá adotar procedimentos visando certificar-se de que a empresa contratada atende as seguintes exigências:

- **Adoção de práticas de Governança Corporativa e de Gestão proporcionais a relevância dos serviços que estão sendo contratados e aos riscos que estão expostos, como por exemplo:**

  - Se mantém Política de Segurança Cibernética e da Informação;
  - Se possui Plano de Continuidade Operacional;
  - Se as mudanças ou alterações de serviços ou sistemas são registradas e autorizadas quando de sua implantação em produção (Gestão de Mudanças);
  - Se mantém Gestão de Incidentes.

- **Verificação da capacidade do potencial Prestador de Serviços de forma a assegurar os seguintes requisitos:**

  - Cumprimento da legislação e da regulamentação em vigor;

- Permissão de acesso da cooperativa aos dados e as informações a serem processadas ou armazenadas pelo Prestador de Serviços;
- Confidencialidade, Integridade, disponibilidade e recuperação dos dados e das Informações processadas ou armazenadas pelo Prestador de Serviços;
- Aderência a certificações que a cooperativa possa exigir para a prestação do serviço a ser contratado;
- Acesso da cooperativa aos relatórios elaborados por empresa de Auditoria especializada independente contratada pelo Prestador de Serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados;
- Provimento de informações e de recursos de Gestão adequados ao monitoramento dos serviços a serem prestados;
- Identificação e segregação dos dados dos clientes da cooperativa por meio de controles físicos e lógicos;
- Qualidade dos controles de acesso voltados à proteção dos dados e das informações dos cooperados.

09 - AVALIAÇÃO DOS SERVIÇOS A SEREM CONTRATADOS

A CRETOVALE, 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;

b. o acesso da cooperativa 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 cooperativa 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 cooperativa 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 cooperativa; e

i. Necessidade de acesso às informações/dados pelo Banco Central do Brasil.

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

iv. 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.

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;

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

10 - DOS CONTRATOS

Os contratos firmados entre a cooperativa e as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

a) A indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, quando houver;
b) A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
c) A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;
d) A obrigatoriedade, em caso de extinção do contrato, de:

- Transferência dos dados ao novo prestador de serviços ou à cooperativa.
- Exclusão dos dados pela empresa contratada substituída após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.

e) O acesso da cooperativa à:

- Informações fornecidas pela empresa contratada visando o cumprimento dos itens previstos nos itens a b e c acima;
- Informações relativas às Certificações exigidas pela cooperativa e aos relatórios de auditoria especializada contratada pelo prestador de serviços;
- Informações e recursos de Gestão adequados ao monitoramento dos serviços prestados.

f) A obrigação da empresa contratada de notificar a cooperativa sobre a subcontratação de serviços relevantes para a contratada.
g) A permissão de acesso do Banco Central às seguintes informações:

- Contratos e acordos firmados para a prestação de serviços;
- Documentação e informações referentes aos serviços prestados;
- Os dados armazenados;
- As informações sobre processamentos;
- As cópias de segurança dos dados e das informações;
- Códigos de acesso aos dados e as informações.

h) A adoção de medidas pela cooperativa em decorrência de determinação do Banco Central.

i) A obrigatoriedade da empresa contratada de manter a cooperativa permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e regulamentação em vigor.

j) O contrato deve também prever, para o caso de decretação de regime de resolução da cooperativa pelo Banco Central:

- A obrigação da empresa contratada para a prestação de serviços concederem pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, a documentação e as informações referentes aos serviços prestados, aos dados armazenados e as informações sobre seus processos, as cópias de segurança dos dados e das informações, bem como aos códigos de acesso que esteja em poder da empresa contratada;
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção da empresa contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observando que:

  - ✓ A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, realizado pelo responsável pelo regime da resolução.
  - ✓ A notificação prévia deve ocorrer também na situação em que a interrupção for motivada por inadimplência da cooperativa.

11 - COMUNICAÇÃO AO BANCO CENTRAL

A Cooperativa deverá informar previamente ao Banco Central a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.
Essa comunicação deve ser realizada até dez dias após a contratação dos serviços e deve conter as seguintes informações:

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

As alterações contratuais que impliquem modificações nas informações contratuais devem ser comunicadas ao Banco Central no mínimo 60 dias antes da alteração contratual.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a ser realizada pela cooperativa quando houver, deve observar os seguintes requisitos:

- A existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
- Assegurar que a prestação dos serviços não cause prejuízo ao seu regular funcionamento nem embaraço a atuação do Banco Central do Brasil;
- Definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e
- Prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de inexistência de convênio citado nos itens anteriores a cooperativa deverá solicitar autorização do Banco Central para a contratação, observando o prazo e as informações já mencionadas.

A Cooperativa deve assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições contratantes e do Banco Central do Brasil e às informações.

12 - CONTROLES DA SEGURANÇA CIBENÉRTICA E DA INFORMAÇÃO

A CRETOVALE estabeleceu plano de ação e de resposta a incidentes visando a implantação da Política de Segurança Cibernética e da Informação aprovado pela Diretoria.

São exigidos alguns controles básicos de segurança da informação:

a) Política de Segurança Cibernética e da Informação e respectivo 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 cooperativa, 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 e da informação, pela execução do plano de ação e pela gestão de incidentes;
f) Implementação de programas de capacitação em segurança;
g) Comunicação para clientes e usuários;
h) Comprometimento da alta administração.

13 - 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 cooperativa - **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:

a) 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;
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.

É importante ressaltar a cooperativa de informar ao Banco Central do Brasil (BCB) os incidentes relevantes conforme demais instruções publicadas na Resolução CMN nº 4.893/21.

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 (tempo razoavelmente considerável);
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;
vi. ataques DDOS, entre outros.

14 - PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

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

I. as ações a serem desenvolvidas pela cooperativa para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política;
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; 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;
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; e
III. 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.

Relatório de Testes de Segurança das Informações

Sempre que solicitado pela cooperativa, o departamento de TI da empresa contratada, 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. Todas as informações são prestadas pela empresa em relatório anual.

Estes testes serão realizados pela equipe de suporte de TI da empresa 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 a 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 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;
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.

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 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.

Divulgação da Política de Segurança Cibernética e da Informação

A política de segurança cibernética e da informação será divulgada aos colaboradores da cooperativa e às empresas prestadoras de serviços através da página da cooperativa na internet, podendo, a seu critério, considerar tais informações no contrato de prestação de serviço, quando necessário.

15 - CONSIDERAÇÕES FINAIS

A CRETOVALE deverá: designar diretor responsável pelo cumprimento da Política de Segurança Cibernética e da Informação, e pela execução do plano de ação e de resposta a incidentes, que pode desempenhar outras funções na cooperativa, desde que não haja conflito de interesses.

A Política de Segurança Cibernética e da informação será aprovada e revisada a cada 2 (dois) anos pela Diretoria ou quando houver exigências / alterações dos órgãos normativos, após revisão deverá ser realiza sua divulgação, bem como manter toda a documentação relativa a este regulamento à disposição do Banco Central do Brasil.

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

Eu, _____, inscrito no CPF/MF sob o nº _____, declaro que li e estou plenamente de acordo com as disposições da Política de Segurança das Informações e de Segurança Cibernética aprovados pela CRETOVALE em ..... Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

Local e data

_____

Assinatura

Nome:

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.

(*)

Severidade Alta: quando o Incidente tem um impacto elevado nas atividades da cooperativa, comprometendo o seu funcionamento e ao ponto de causar prejuízos;
Severidade Média: quando o Incidente tem um impacto significativo, podendo evoluir, mas não chega a gerar prejuízos; e
Severidade Baixa: quando o Incidente é pequeno, não causa prejuízos, mas pode evoluir e ter um impacto significativo nas atividades da cooperativa

(**)

Confidencialidade: toda informação deve ser protegida tendo em vista a sua característica e considerando o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas a quem é destinada.
Integridade: toda informação deve ser mantida na condição em que foi disponibilizada pelo seu titular, visando protegê-la contra alterações indevidas, intencionais e acidentais.
Disponibilidade: toda informação gerada ou adquirida por um indivíduo ou instituição, deve estar disponível aos seus usuários quando eles necessitarem delas para qualquer finalidade.