POLÍTICA DE RISCO CIBERNÉTICO

ServiCOOP

Instituição Financeira Cooperativa

CONSELHO DE ADMINISTRAÇÃO

SERVICOOP

OUTUBRO DE 2022

ATUALIZAÇÕES

Abaixo relacionamos as alterações procedidas nesta Política.

Data	Responsável	Assunto
Outubro 2022	Diretoria de Tecnologia da Informação	Criação da Política de Risco Cibernético

SUMÁRIO

1. OBJETIVO

Estabelecer 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 Cooperativa. 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.

2. ABRANGÊNCIA

A presente Política é aprovada pelo Conselho de Administração e abrange todas as áreas da Cooperativa.

3. DIRETRIZES GERAIS

A informação é um ativo essencial para os negócios e controles da Cooperativa, devendo ser adequadamente tratada e protegida. Isto é especialmente importante em um ambiente de negócios cada vez mais interconectado.

Segurança cibernética e da informação é a proteção das informações contra diversos tipos de ameaças, a fim de minimizar a exposição a riscos, garantindo que sejam preservadas as características fundamentais de confidencialidade, integridade, disponibilidade e conformidade de informações sensíveis. O arcabouço de ferramentas e processos adotados pela Cooperativa visa proteger contra o vazamento de informações e fraudes, zelar pela privacidade, garantir que sistemas e informações estejam disponíveis para a continuidade de negócios, bem como zelar pela proteção da imagem e credibilidade da Cooperativa junto a seus associados e comunidade em geral.

A Cooperativa, por meio de responsável pela Tecnologia da Informação e de forma alinhada com os objetivos e requisitos do negócio, estabelece nesta Política de Segurança Cibernética e da Informação, regras e direcionamentos a serem seguidos e

aplicados a pessoas, processos e tecnologia, de forma a proteger suas informações, de seus associados, clientes, fornecedores e parceiros de negócios.

3.1. DEFINIÇÕES

Para efeito deste documento, aplicam-se os seguintes termos e definições.

3.1.1. Recursos

Qualquer recurso, tangível ou intangível, pertencentes, a serviço ou sob responsabilidade da Cooperativa, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.

3.1.2. 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.

3.1.3. Boas Práticas de Segurança da Informação

São consideradas boas práticas de segurança da informação as recomendações contidas em normas e instituições como: ISO/IEC 27001, ISO/IEC 31000, OWASP (www.owasp.org), NIST (www.nist.gov), ISACA (www.isaca.com.br), SANS (www.sans.org) e outras internacionalmente reconhecidas.

3.1.4. Colaborador

Entende-se como Colaborador qualquer pessoa que trabalhe para a Cooperativa, quer seja: Funcionário com registro em carteira de trabalho, terceiro, estagiário, aprendiz ou trainee.

3.1.5. 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.

3.1.6. Gestor

Colaborador que exerce cargo de liderança, como: presidente, vice-presidente, diretor, gerente, coordenador, líder ou chefe de seção.

3.1.7. IDS

Intrusion Detection System ou Sistema de Detecção de Intrusão é uma ferramenta utilizada para monitorar o tráfego da rede, detectar e alertar sobre ataques e tentativas de acessos indevidos.

3.1.8. IPS

Intrusion Prevention System ou Sistema de Prevenção de Intrusão é uma ferramenta que tem a capacidade de identificar uma intrusão, analisar a relevância do evento/risco e bloquear determinados eventos, fortalecendo assim a tradicional técnica de detecção de intrusos.

3.1.9. Informação

Qualquer conjunto organizado de dados que possua algum propósito e valor para a Cooperativa, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, estar sob sua custódia ou sob custódia de terceiros, como por exemplo, informações armazenadas em nuvem.

3.1.10. Princípios de "*Least Privilege*" e "*Need to Know*"

Estes princípios devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de acesso (*Least Privilege*) a quem realmente tenha a necessidade de acesso (*Need to Know*).

3.1.11. Política de Segurança Cibernética e da Informação

Estrutura de documentos formada pela Política, normas e padrões de segurança cibernética e segurança da informação.

3.1.12. 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.

3.2. Segurança da Informação (SI)

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

- **Confidencialidade:** garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;
- **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.
- **Disponibilidade:** garantia de que os Colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessários, nos períodos e ambientes aprovados pela empresa;
- **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.

3.3. 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.

3.4. Recursos Críticos

Recursos essenciais para o funcionamento da operação da Cooperativa e que possuem informações críticas ou sensíveis.

3.5. Baselines

Requisitos, recomendações e melhores práticas de configurações de segurança da informação para os ativos.

3.6. 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.

4. DIRETRIZES ESPECÍFICAS

4.1. Aquisição, Desenvolvimento e Manutenção de Tecnologia da Informação.

Aquisições, desenvolvimento, contratações e a manutenções de Tecnologia da Informação devem ser centralizadas e gerenciadas pela área de Tecnologia da Informação da Cooperativa.

Os responsáveis pela aquisição de produtos ou serviços de Tecnologia da Informação, assim como o desenvolvimento e manutenção de ativos tecnológicos, devem:

- Garantir a adoção e manutenção dos requisitos previamente definidos nas *baselines*, padrões e normas de segurança da informação;
- Garantir a validação de requisitos de Segurança da Informação na análise crítica de novas soluções ou para aquelas que sofreram alterações significativas;
- Garantir o atendimento aos requisitos de segurança necessários para assegurar a confidencialidade, integridade, disponibilidade e conformidade de sistemas e informações;
- Garantir que novas soluções sejam devidamente documentadas, assim como mantida documentação para entendimento e rastreabilidade das ações realizadas.

Os Recursos de Tecnologia da Informação utilizados pela Cooperativa devem ser inventariados, controlados e colocados à disposição, de acordo com as regras de acesso vigentes.

Na contratação de serviços, os contratos firmados entre as partes e a Cooperativa devem conter cláusulas de confidencialidade, responsabilidade pela proteção da informação, não divulgação e descarte das informações. Outras cláusulas específicas de Segurança da Informação podem ser requeridas de acordo com o contexto do serviço contratado.

O sigilo necessário com as informações da Cooperativa deve perdurar mesmo após o encerramento da prestação de serviços. Este ponto deve ser previsto no estabelecimento de contratos.

A veracidade das informações contidas em contratos deve ser verificada.

4.2. Classificação da Informação

A responsabilidade pelas informações arquivadas ou processadas pela Cooperativa deve ser atribuída a um proprietário formalmente designado.

Toda a informação deve ser classificada, de acordo com seu valor, grau de sigilo, criticidade e sensibilidade perante o negócio, de forma que sejam adotados os mecanismos de proteção adequados, balanceando custo e complexidade do controle.

Informações sem classificação explícita devem ser consideradas como “Interno”, não sendo permitido o seu repasse ou divulgação para qualquer pessoa que não seja da Cooperativa, exceto informações públicas e de mercado, devidamente autorizadas.

Todos os Colaboradores devem tratar as informações da Cooperativa de acordo com seu nível de classificação de forma a protegê-las contra atos ou acessos indevidos ou divulgação não autorizada, mantendo sua confidencialidade, integridade e disponibilidade.

4.3. Comportamento Seguro

i. Os recursos e as informações de propriedade ou sob custódia da Cooperativa devem ser utilizados de acordo com os interesses da organização, para prestação dos seus serviços, atendendo aos requisitos e respeitando as regras estabelecidas.

ii. Independente dos meios onde a informação esteja armazenada ou onde seja transmitida, cada Colaborador deve assumir um comportamento seguro e proativo impedindo seu vazamento para pessoas ou meios externos da Cooperativa.

iii. Aos Colaboradores, sem autorização prévia, é vetado emitir opiniões em nome da Cooperativa ou utilizar informações privadas da Cooperativa em: e-mails, sites, redes sociais, publicações impressas, fóruns de discussão, serviços da Internet e outros ambientes públicos, em face da possibilidade de divulgação inadvertida.

iv. O uso da marca, nome ou citação da Cooperativa deve cumprir os requisitos de autorização por direito de imagem e propriedade.

v. Os colaboradores são responsáveis por manter as informações da Cooperativa em locais seguros. Isso se aplica a informações impressas, escritas em quadros ou em outras mídias físicas, que não devem ser deixadas desprotegidas em salas de reuniões, mesas ou qualquer local dentro e fora da empresa.

vi. O descarte de informações internas, restritas ou confidenciais, contidas em qualquer meio, quer seja impresso, eletrônico, magnético, ou sob qualquer outra forma, deve ser feito de forma segura, garantindo a destruição dos dados de forma que não possam ser novamente recuperados.

vii. O uso de recursos tecnológicos para gravação, foto e filmagem de qualquer reunião ou evento corporativo não é permitido sem prévia autorização e consentimento de todos os participantes.

4.4. Conformidade

i. O cumprimento e aderência às leis, regulamentações, Política de Segurança Cibernética e da Informação, normas, obrigações contratuais, e padrões de segurança, são obrigatórios e devem ser garantidos por todos os Colaboradores da Cooperativa.

ii. Responsáveis por recursos críticos da Cooperativa devem garantir a retenção de evidências da execução de seus controles para fornecimento em casos de auditorias ou necessidade do atendimento a regulamentações.

4.5. Conscientização e Divulgação de Segurança Cibernética e da Informação

i. A Política de Segurança Cibernética e da Informação, normas e padrões de segurança devem ser amplamente divulgadas no processo de admissão e integração de novos Colaboradores, tanto pela equipe de Recursos Humanos quanto pelos Gestores.

ii. Programas de conscientização, divulgação e reciclagem do conhecimento da Política de Segurança Cibernética e da Informação devem ser estabelecidos e praticados regularmente para garantir que todos os Colaboradores e terceiros conheçam as diretrizes e responsabilidades relacionadas à segurança das informações.

4.6. Continuidade de Negócios

Deve-se estabelecer, documentar, implantar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para os serviços e processos de negócio da Cooperativa, durante situações adversas.

Como parte integrante desta Política de Risco Cibernético a Cooperativa adota os parâmetros e ações previstas nos Planos de Continuidade de Negócios, Plano de Resposta a Incidentes de Segurança de Informação e Política de Backup e de Recuperação de Processamento, especialmente nos aspectos relativos ao sistema legado de gestão dos produtos e serviços disponibilizados aos associados.

Os planos acima citados apresentam os cenários de indisponibilidade dos serviços, apresentando também as devidas ações para restabelecimento dos serviços, bem como prevendo ações de prevenção a possíveis incidentes.

4.7. Segurança Física

i. Os equipamentos e instalações de processamento de informação críticas ou sensíveis, bem como as próprias informações sensíveis, deverão ser mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

ii. As áreas seguras da Cooperativa devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.

iii. O acesso de qualquer pessoa às instalações da Cooperativa somente deverá ser feito mediante autorização por Colaboradores responsáveis por esse controle e mediante identificação do visitante. Nenhum visitante tem a autorização de circular pelas dependências da Cooperativa sem estar acompanhado por um colaborador Cooperativa.

iv. As recepções e áreas de maior criticidade devem estar sob proteção de um circuito interno de câmeras de vídeo, instaladas em locais estratégicos. As imagens obtidas devem ser preservadas com segurança.

4.8. Acesso Lógico

i. O processo de gestão dos acessos a qualquer sistema da Cooperativa quer seja interno ou em nuvem, deve ser conduzido pela área de TI, exceções deverão ser tratadas junto a alta direção.

ii. O acesso a qualquer sistema tecnológico da Cooperativa deve ser autenticado, ou seja, protegido por credenciais de acesso, certificados, *tokens* ou qualquer outro método seguro de identificação e autenticação.

iii. Acessos a informações e a sistemas da Cooperativa devem ser permitidos apenas após dois ou mais níveis de autorização, sendo o primeiro do gestor do colaborador solicitante e o segundo do responsável pela informação ou sistema.

iv. Os acessos de colaboradores e terceiros devem ser desativados assim que desligados ou encerrados contratos de prestação de serviços.

v. As credenciais de acesso a sistemas e informações, compostas por usuário e senha, são concedidas pela Cooperativa aos Colaboradores e Terceiros para uso em atividades relacionadas a seu trabalho, pelo tempo em que perdurar seu vínculo com a empresa.

vi. É proibido transferir, compartilhar, emprestar ou revelar a senha das credenciais de acesso concedidas pela empresa a outros colaboradores, assim como é proibido o uso de credenciais de outros colaboradores.

vii. Todos os perfis de usuários e acessos a informações ou sistemas de média e alta criticidade devem ser revisados periodicamente pelo respectivo responsável, seguindo os critérios de segregação da função e observando o princípio de mínimo acesso (*least privilege*) e necessidade de conhecimento (*need to know*).

4.9. Gestão de risco de Segurança da Informação

i. A Gestão de Riscos de Segurança da Informação deve ser realizada através de um processo estruturado que contemple a identificação, análise, avaliação, priorização, comunicação, tratamento e monitoração dos riscos que podem afetar negativamente os negócios da organização.

ii. O processo de gestão de riscos deve contemplar novos ativos, sistemas ou processos, quer sejam eles internos, em nuvem ou conduzidos por parceiros.

4.10. Incidentes de Segurança da Informação

i. São considerados incidentes de segurança da informação quaisquer eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de Segurança da Informação: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio em risco.

ii. Violações ou tentativas de violação desta Política, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

iii. Colaboradores devem informar imediatamente à segurança da informação todas as violações à Política de segurança da informação, normas, padrões incidentes ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

iv. A identificação de incidentes de segurança pode ocasionar o bloqueio imediato dos acessos dos colaboradores envolvidos até que sejam concluídas as investigações necessárias.

v. A ocorrência de incidentes de segurança de informação que signifiquem acesso relevante a dados dos associados ou que representem interrupção dos serviços e atendimento aos associados, por período superior a 48 (quarenta e oito) horas deverá ser comunicada de imediato ao Banco Central do Brasil por meio dos devidos canais disponibilizados por esta autarquia.

vi. Cabe à cooperativa criar canais com as demais instituições financeiras para, de forma corporativa, compartilhar informações quanto aos incidentes previstos no item anterior.

4.11. Monitoramento

i. Todas as ações de colaboradores e visitantes, realizadas nas dependências da Cooperativa ou remotamente, abrangendo o acesso físico e a utilização de recursos de tecnologia da informação e comunicação do grupo, podem ser monitoradas.

ii. A área de TI é responsável por garantir a privacidade dos registros oriundos da monitoração do acesso e uso de sistemas e serviços de Tecnologia da Informação.

iii. Ao acessarem sistemas e recursos tecnológicos da Cooperativa, Colaboradores e visitantes concordam que suas ações podem ser monitoradas.

iv. Os registros obtidos através de monitoramento poderão ser utilizados em processos de investigação de incidentes e suspeitas de violação de leis e de Normas do Grupo, bem como, em processos judiciais e trabalhistas, a critério da Cooperativa.

v. Tendo em vista ao encontro de incidentes de segurança de informação, conforme previsto nesta Política e nos Planos anexos, cabe ao setor de TI desenvolver, de imediato, documento detalhando o incidente e as ações tomadas ou a serem implantadas com vistas a resolver o problema e evitar que o mesmo venha a se repetir no futuro.

4.12. Privacidade

i. Deve-se assegurar a privacidade e a proteção, conforme previsto pela legislação e regulamentação pertinente, todas as informações pessoais de clientes, colaboradores, parceiros de negócio e outras que venham a ser armazenadas, processadas ou colocadas sob custódia da Cooperativa.

4.13. Propriedade Intelectual

i. A Cooperativa é proprietária ou custodiante responsável por toda a informação criada, armazenada, transmitida, transportada, processada ou descartada pelos seus recursos ou por aqueles contratados pela Cooperativa em nuvem ou prestados por terceiros devidamente autorizados.

ii. É proibida aos Colaboradores a violação da propriedade intelectual do grupo ou de terceiros, quer seja por meio da utilização indevida de imagens, textos, softwares, marcas ou pela cópia indevida de originais ou conversão do formato destes.

4.14. Utilização de Recursos de Tecnologia da Informação

i. Para utilização de qualquer recurso de tecnologia da informação é necessária a aprovação prévia do gestor do colaborador/terceiro e do proprietário da informação, sistema ou recurso.

ii. Não é permitida aos Colaboradores e Terceiros a instalação de qualquer software ou a alteração de parâmetros de configuração de computadores da Cooperativa. Estas devem ser realizadas por equipes de TI autorizadas, após processos de homologação e obtenção do licenciamento adequado. Softwares instalados indevidamente poderão ser automaticamente excluídos, sem prévio aviso.

iii. É proibido o armazenamento, transmissão, processamento e impressão de conteúdo que contenha pedofilia, pornografia, erotismo, violência, terrorismo, racismo, intolerância, e outros conteúdos proibidos por leis, moral, ética e normas da Cooperativa.

iv. As informações internas, restritas e confidenciais ou sensíveis da Cooperativa não devem ser copiadas, sincronizadas ou replicadas em serviços em nuvem, exceto situações analisadas e aprovadas pela alta direção.

v. Informações da Cooperativa ou sob sua custódia e responsabilidade, somente podem ser transportadas ou processadas em meios previamente aprovados pela alta direção, a exemplo e-mail pessoal, Internet, pendrive, redes sociais, CD/DVD, papel, computador pessoal dentre outros meios.

vi. O acesso de celulares, smartphones, tablets e qualquer outro dispositivo a serviços e informações da Cooperativa deve ser permitido apenas após o atendimento integral dos requisitos de segurança da Cooperativa definidos nas normas para esta categoria de dispositivos.

vii. Documentos eletrônicos de uso da Cooperativa devem ser armazenados em repositórios centralizados da rede (servidores de arquivos) com as devidas proteções de segurança, dentre elas: controle de acesso e backup. Documentos eletrônicos do grupo não devem ser armazenados em estações de trabalho.

viii. Os colaboradores devem zelar pela segurança de ativos da empresa colocados sob sua responsabilidade, como dispositivos móveis e notebooks.

ix. O uso de recursos de criptografia deve ser autorizado pela área de TI e estar de acordo com os padrões definidos para a Cooperativa

4.15. Segurança em Redes

i. Devem existir controles tecnológicos para proteger o acesso entre redes (incluindo Internet, redes públicas, extranets, acesso remoto, wireless e as diferentes redes de usuários).

ii. Equipamentos com diferentes requerimentos de segurança devem ser segregados em redes diferentes.

iii. Além do controle de acesso entre as redes, deve ser protegida a informação em trânsito, seguindo os requerimentos da Classificação da Informação.

iv. O acesso remoto somente será permitido para situações onde for indispensável e esteja documentado e com mecanismos de autenticação de dois fatores.

v. Os níveis de segurança (confidencialidade, integridade e disponibilidade) esperados dos serviços de comunicações, devem ser estabelecidos nos contratos firmados com os fornecedores desses serviços.

vi. Deve ser implementado controle tecnológico de Firewall para a proteção das redes mais críticas.

vii. Controles criptográficos devem ser solicitados, estabelecidos e/ou desenvolvidos, para garantir os níveis de confidencialidade das informações trafegadas, segundo a sua classificação (definido pelo proprietário da informação).

4.16. Registros de Auditoria

i. Todas as ações de usuários, sistemas e qualquer evento de Segurança da Informação devem gerar trilhas de auditoria (logs), que deverão ser mantidos por um período mínimo de 5 anos, em local centralizado e protegido contra acessos não autorizados.

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

iii. Todo acesso de consulta, cópia ou tentativa de modificação e exclusão as trilhas de auditoria (logs) devem ser registradas.

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

4.17. Backups, arquivamento e restaurações

i. A área de TI deve determinar os recursos requeridos para cumprir com os requerimentos mínimos de respaldo dos ativos de informação, conforme definido pelos proprietários da informação.

ii. A área de TI deverá estabelecer um plano de backup para cumprir com esses requisitos e deverá estabelecer mecanismos para a correta execução das rotinas de backup.

iii. Diariamente devem ser validados os resultados da realização dos backups, sendo que as falhas deverão ser reportadas como incidente de segurança.

iv. O processo de backup e restauração para todos os sistemas deve ser testados em intervalos regulares, com o objetivo de assegurar que estejam em conformidade com os requerimentos dos donos da informação e com as exigências do plano de continuidade do negócio da companhia.

v. O tempo necessário que a informação deve ser mantida deverá estar de acordo com as necessidades do negócio e deve levar em consideração as exigências das leis vigentes.

4.18. Análise de Vulnerabilidades Técnicas

i. Periodicamente devem ser realizados testes de vulnerabilidades técnicas dos equipamentos críticos da infraestrutura.

ii. Após os levantamentos, as comparações e identificações dos riscos devem ser executadas, possibilitando o tratamento dos riscos de acordo com seus níveis.

iii. Nos casos em que não for possível a eliminação total da vulnerabilidade, deve ser apresentada aceitação do risco ou a determinação de falso positivo.

iv. Verificações ou auditorias regulares devem verificar a conformidade com as exigências técnicas dos sistemas e das redes.

v. As auditorias realizadas por terceiros devem identificar claramente as interações com os sistemas em operação.

vi. As auditorias técnicas dos sistemas e das redes devem respeitar as práticas estabelecidas e devem ser realizadas de acordo com as recomendações da organização. Estas auditorias devem ser realizadas por fornecedores reconhecidos e competentes.

4.19. Prevenção, Detecção de Intrusão

i. Todos os recursos do sistema de informação expostos à Internet devem ser acompanhados e protegidos por um IDS / IPS.

ii. Sempre que o IDS / IPS detecta ou responde a uma tentativa externa mal-intencionada suficientemente grave para ameaçar os recursos do sistema de informações protegidas, uma análise estruturada e procedimento de resposta deve ser acionado.

4.20. Proteção contra códigos maliciosos

i. Deverão ser implementados controles tecnológicos para a proteção dos equipamentos de processamento de informação que executem algum tipo de software (tanto de usuário final como servidores) para a prevenção, detecção, correção e erradicação de códigos executáveis maliciosos.

ii. Deve ser verificada a atualização das ferramentas de proteção baseadas em assinaturas, para que estejam nas últimas atualizações disponíveis.

4.21. Troca de Informações

i. A transmissão digital de informações através de canais de comunicação não seguros deve ser protegida de acordo com o nível da classificação da informação, especialmente analisando a necessidade de utilização de criptografia para a proteção da informação.

ii. A transmissão física de informações digitais deve ser protegida segundo a classificação da informação. Rótulos, lacres, assinaturas e criptografia devem ser considerados.

iii. O estabelecimento de comunicações entre redes protegidas com parceiros (Extranets) deve ser protegido por mecanismos criptográficos, ou outros mecanismos similares para proteger a confidencialidade e integridade da informação.

iv. As áreas de negócio devem sempre utilizar os canais de comunicação seguro (STCP, VPN, SSH, etc.) para envio e recebimento de informações confidenciais entre parceiros e fornecedores, quando possível. Quando não for possível utilizar esse canal a informação deve ser protegida com criptografia ou senha forte, para evitar vazamento das informações.

4.22. Controles Criptográficos

i. Deverão ser utilizados controles criptográficos para proteger as informações segundo os requerimentos da sua classificação.

ii. Somente algoritmos de criptografia aprovados pela área de TI podem ser utilizados nas soluções e sistemas adotados pela Cooperativa.

iii. O gerenciamento das chaves de criptografia deve prever mecanismos para o armazenamento seguro, geração segura da chave e destruição da chave.

iv. Deverá existir um mecanismo de recuperação da informação caso seja perdida uma chave de criptografia.

v. As chaves de criptografia devem ser trocadas periodicamente, dependendo da sua frequência de utilização.

vi. Caso seja comprometida uma chave criptográfica, deve ser revogada imediatamente. Se for uma chave para criptografia de arquivos, deve ser trocada.

vii. Mecanismos de autenticação e auditoria devem ser estabelecidos para garantir a segurança do acesso às chaves.

4.23. Aquisição, Desenvolvimento e Manutenção Segura de Sistemas

i. Sistemas da informação desenvolvidos ou adquiridos devem contar com atributos e funcionalidades de segurança que protejam adequadamente as informações. Os requerimentos devem ser identificados e documentados na fase de concepção do sistema, para assegurar que as demandas de segurança sejam atendidas.

ii. Devem ser desenvolvidos controles que previnam erros de operação, perda, ou vazamento de informações. Todo sistema deve ser documentado, tornando sua implantação e operação independente de conhecimentos informais.

iii. Devem ser estabelecidos controles criptográficos para proteger a confidencialidade, autenticidade ou integridade das informações. Faz-se necessária a documentação do uso de chaves, quando necessário.

iv. Sistemas devem ser protegidos contra alteração indevida, evitando a exposição de dados sensíveis. Devem ser estabelecidos controles para monitorar e corrigir as vulnerabilidades e falhas desses.

v. O acesso ao código fonte das aplicações deve ser protegido, seguindo as características definidas pela classificação da informação.

vi. Somente colaboradores autorizados devem ter acesso ao código-fonte, com os correspondentes controles de versão.

vii. As instalações de desenvolvimento, teste e produção devem ser separadas. Deve haver segregação entre estes ambientes para evitar que dados de um ambiente sejam utilizados em outro.

viii. Dados reais de produção não serão utilizados para testar aplicativos.

ix. Dados privados de usuários não serão utilizados para testar aplicativos.

x. Deverá ser assinado um termo de confidencialidade assim como assinadas as políticas de segurança por parte de terceiros que façam desenvolvimento de sistemas para a Cooperativa.

xi. O desenvolvimento de sistemas por parte de terceiros deverá ser controlado e auditado por pessoal técnico da Cooperativa.

xii. O desenvolvimento de sistemas deverá seguir as boas práticas de mercado quanto ao Desenvolvimento Seguro.

xiii. Toda manutenção em sistemas deve:

a. Considerar os requerimentos de segurança antes, durante e depois da manutenção;

b. Garantir a integridade e a conformidade das especificações funcionais iniciais;

c. Respeitar a consistência e a homogeneidade do nível de segurança estabelecido inicialmente no desenvolvimento da aplicação;

d. Respeitar, ao efetuar as modificações, os resultados da análise inicial do risco realizada na fase de projeto;

e. Garantir a origem e a integridade das entregas para o ambiente de produção;

f. Preservar a confidencialidade dos contextos operacionais;

g. Preservar a segurança dos sistemas ou da rede, assegurando que nenhuma intervenção forneça a oportunidade de sabotagens de forma inesperada ou de ações maliciosas;

h. Respeitar as obrigações legais e contratuais com relação à confidencialidade das informações processadas pelos sistemas.

4.24. Serviço de Nuvem

i. A possibilidade de utilização de uma solução de hospedagem externa, e, mais especificamente, uma solução '*cloud computing*', depende do nível de sensibilidade dos dados e os processos em questão. Esta escolha deve ser feita com base em uma análise de risco.

ii. Toda e qualquer contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverá ser previamente comunicada ao Banco Central do Brasil.

iii. Os serviços para processamentos de dados e ou armazenamento em nuvem, sejam eles software como serviço (SaaS) ou armazenamento de base de dados devem possuir acesso seguro através de interfaces HTTPS bem como a autenticação segura e em ambientes segregados.

iv. Os acessos devem ser controlados por meio de logins e senhas individuais, previamente fornecidos, de acordo com a atividade de cada colaborador/terceiro ou administrador, possuindo também tais acessos e ações registrados em trilhas de auditorias.

4.25. Gestão de Incidentes de Segurança

i. Qualquer evento relacionado a um suposto ou comprovado ataque a segurança de um sistema operacional deve ser resolvido de acordo com um processo de gerenciamento de incidentes.

ii. Os procedimentos envolvidos devem descrever o processo de gerenciamento de incidente, o processo de investigação e o processo de recolhimento de provas. O processo de gerenciamento de incidente deve:

a. Permitir a detecção, o mais cedo possível, e a capacidade de responder com a máxima eficácia para limitar os danos causados pelo incidente;

b. Limitar as zonas de vulnerabilidade pela remediação de anomalias identificadas em algum ou todos os sistemas operacionais potencialmente afetados;

c. Reter informações relevantes para posteriores investigações e coleta de provas;

d. Compilar um registro de incidentes de segurança e estatísticas para uso na previsão de possíveis incidentes futuros;

e. Identificar pontos de contato apropriados para o nível de severidade do ataque

iii. Uma vez que um incidente mal-intencionado for resolvido, uma análise deve ser feita para identificar a origem do ataque e iniciar procedimentos administrativos ou judiciais apropriados.

iv. Cabe a cada setor da cooperativa, sempre que identificar um incidente de segurança de qualquer dos sistemas utilizados pela Cooperativa, encaminhar um comunicado formal à gerência da Cooperativa e ao setor de Controles Internos no sentido de registrar tal ocorrência.

v. Cabe à gerência da Cooperativa, em conjunto com o responsável pela TI, acionar, seguindo os procedimentos estabelecidos nos Planos de Continuidade de Negócios e Respostas a Incidentes de Segurança da Informação, os responsáveis pelos controles de segurança dos respectivos sistemas para resolução imediata e implementação de ações que evitem futuras repetições de possíveis incidentes detectados.

vi. O Setor de Controles Internos da Cooperativa deverá registrar, contendo inclusive causa e impacto, as informações e encaminhamentos dados no sentido de solucionar os possíveis incidentes de segurança detectados. Os registros deverão compor relatório do setor a ser apresentado semestralmente ao Conselho de Administração e Fiscal da Cooperativa.

4.26. Gestão de Fornecedores

i. O gerenciamento de fornecedores deverá considerar a avaliação de risco e classificação dos fornecedores (estratégico, tático, operacional).

ii. A intervalos regulares o desempenho dos fornecedores críticos deve ser medido quanto ao cumprimento das metas acordadas e os resultados avaliados. Os resultados devem ser discutidos com o fornecedor para se identificar as necessidades e oportunidades de melhoria.

iii. Cada fornecedor deverá ter um gestor designado que acompanha o seu desempenho, tornando-o responsável pela qualidade dos serviços fornecidos.

4.27. Atualizações desta e demais políticas

i. Esta Política está sujeita a revisões anuais, podendo ser revisada em periodicidade menor, caso necessário, em decorrência de alterações na regulamentação e/ou legislação aplicável ou, ainda, para refletir alterações nos procedimentos internos da organização.

ii. Esta e demais políticas passarão pelo seguinte procedimento de elaboração e revisão:

a) Gestor responsável pela alteração solicitada e/ou inclusão de novo procedimento na política;

b) Avaliação e aprovação do Diretor responsável por esta Política.

c) A versão atualizada desta Política será publicada na Internet e Intranet e deverá ser lida por todos os colaboradores.

5. APLICABILIDADE

i. O Gestor imediato ou a alta direção deve ser consultado sempre que existir alguma dúvida referente à aplicabilidade da Política de Segurança Cibernética e da Informação e demais documentos que a compõe.

ii. Cabe à área de TI avaliar os riscos de ações não previstas na Política de Segurança Cibernética e da Informação, se necessário levando o assunto a alta direção.

iii. Exceções às diretrizes contidas neste documento e nos demais que compõem a Política de Segurança Cibernética e da Informação devem ser autorizadas pela alta direção.

6. RESPONSABILIDADES

Todo Colaborador, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações da Cooperativa e deve cumprir as determinações da Política, normas e padrões de segurança da informação.

i.Alta Direção

- Prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação.
- Prover comprometimento e apoio à aderência a Política de Segurança Cibernética e da Informação de acordo com os objetivos e estratégias de negócio estabelecidas para organização;
- Fornecer à área responsável pela Segurança da Informação claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário.
- Identificar requisitos legais pertinentes à segurança da informação;
- Garantir a adoção de cláusulas pertinente à segurança das informações nos contratos estabelecidos com a Cooperativa.

ii.Colaborador

- Utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de TI;
- Notificar a área de TI sobre as violações da Política de Segurança Cibernética e da Informação e sobre os incidentes de segurança que venha a tomar conhecimento;
- Manter o sigilo das informações que tenha obtido acesso enquanto Colaborador da Cooperativa, mesmo após seu desligamento da empresa.

iii.Gestor

- Apoiar e incentivar o estabelecimento da Política de Segurança Cibernética e da Informação na Cooperativa;
- Garantir que seus subordinados tenham acesso e conhecimento desta Política e demais normas e padrões de segurança da informação;
- Fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança das informações da Cooperativa;
- Avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;
- 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;
- Acionar as áreas competentes para a aplicação das penalidades, cabíveis aos Colaboradores que violarem a Política de Segurança Cibernética e da Informação e as normas da Cooperativa;
- Autorizar acessos de seus colaboradores apenas quando forem realmente necessários e segundo os conceitos de *need to know* e *least privilege*.

iv.Área de Infraestrutura

- Orientar e coordenar as ações de segurança da informação, promovendo a execução de acordo com o que foi estabelecido;
- Desenvolver e estabelecer programas de conscientização e divulgação da Política de Segurança Cibernética e da Informação;
- Conduzir o processo de Gestão de Riscos de Segurança da Informação;
- Conduzir a Gestão de Incidentes de Segurança da Informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

- Conduzir os processos de monitoração e segurança da informação;
- Definir controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de SI;
- Propor projetos e iniciativas para melhoria do nível de segurança das informações da Cooperativa.
- Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de hardware e software;
- Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia;
- Conduzir a gestão dos acessos a sistemas e informações da Cooperativa;
- Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;
- Informar imediatamente a alta direção, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos da Cooperativa;
- Controlar alterações em ativos de TI e garantir que estas sejam analisadas criticamente e testadas para que não ocorram impactos adversos na operação da empresa ou em sua segurança;
- Garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio.
- Garantir que todos os ativos críticos de Tecnologia da Informação devem ser instalados em ambientes especializados conhecidos como Datacenters. Estes devem conter todas as proteções e contingências necessárias para a sua respectiva proteção.

- Monitorar o acesso físico de Colaboradores às instalações do GPA;
- Administrar o controle de acesso físico.

v.Recursos Humanos

- Verificar o histórico de candidatos a emprego, de acordo com a ética e leis vigentes;
- Garantir que a Política, Normas e Procedimentos da Política de Segurança Cibernética e da Informação sejam divulgados no processo de admissão/integração de novos Colaboradores.

vi.Fornecedores e Parceiros de Negócios

- Cumprir as determinações da Política, Normas e Procedimentos publicados pela Cooperativa;
- Orientar os funcionários da empresa sobre o cumprimento das determinações da Política, Normas e Procedimentos publicados pela Cooperativa;
- Cumprir com o acordo de confidencialidade.

7. PENALIDADES

O Colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração ao Gerente de Infraestrutura. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

8. PLANOS DE CONTINUIDADE DE NEGÓCIOS E RESPOSTA A INCIDENTES DE SEGURANÇA DE INFORMAÇÃO

A Cooperativa possui os seguintes sistemas de informação, sujeitos ao controle desta Política:

Sistema	Fornecedor	Dados em Processamento
Fácil	Fácil	Sistema legado de gerenciamento de todas as operações e serviços prestados pela Cooperativa. Contempla todos os dados dos associados.
Página da Cooperativa na Internet	Locaweb	Página da Cooperativa na Internet. Exposição de documentos institucionais da cooperativa, sem acesso a banco de dados do sistema legado.
Serviço de E-mails	Locaweb	Gerenciamento de correio eletrônico dos funcionários e dirigentes da cooperativa.

Cabe à Gerência da Cooperativa a aplicação de todas as atividades previstas nos Planos de Continuidade de Negócios e Resposta de Incidentes de Segurança de Informação elaborados pelos fornecedores dos serviços listados nesta seção da Política de Risco Cibernético.

Os referidos Planos são parte integrante desta Política e indicam as ações a serem adotadas pelos setores responsáveis na Cooperativa.

8.1. Cenários a serem verificados para continuidade de negócios

Cabe ao setor responsável da cooperativa, conforme listado no quadro abaixo, acompanhar os diferentes cenários para controle e disponibilidade de dados sensíveis a fim de manter a continuidade dos negócios da Cooperativa.

Descrição	Periodicidade	Área Resp.
Criptografia em toda a extensão que possuem alguma exposição com a rede de internet.	Anual	TI
Rotação de senhas e credenciais de acesso dos usuários a seus sistemas e infraestrutura.	Semestral	TI
Teste de stress sobre a camada de Internet Banking.	Trimestral	TI
Teste de integridade de dados	Semestral	TI
Teste de recuperação de desastre	Anual	TI
Troca de informações em ambiente corporativo.	Mensal	Controles Internos
Exigência que o prestador envie a instituição evidência de testes de recuperação de dados sensíveis arquivados e processados em nuvem, bem como de recuperação de dados por desastre em seu ambiente e/ou verificação própria em casos que a administração assim determine.	Semestral	Gerência e empresas terceirizadas
Teste de integridade com amostragem de dados entre o banco de dados em produção e o último backup disponibilizado.	Semestral	Gerência e empresas terceirizadas

Observação

No caso de Colaboradores terceiros, pode ser solicitada às suas respectivas empresas a troca da equipe alocada na Cooperativa, ou ainda, podem ser aplicadas penalidades a empresa tais como, multas, cancelamento do contrato e ações judiciais.

ANEXO I - PLANO DE CONTINUIDADE DE NEGÓCIOS

1. OBJETIVOS

O presente Plano de Continuidade de Negócios é parte anexa à Política de Segurança Cibernética da Cooperativa e visa garantir o funcionamento adequado e pleno da infraestrutura tecnológica existente, bem como serviços de integração com seus parceiros, visando garantir a continuidade dos negócios sensíveis oferecidos a seus associados e/ou clientes.

Os processos e ações decorrentes deste Plano devem garantir a execução de todos os processos críticos dos produtos e serviços oferecidos pela Cooperativa, a fim de manter um processo seguro e eficiente de disponibilidade e processamento de informações.

O plano de continuidade de negócios também objetiva atender às normas e legislação vigentes, que regulam a atuação de instituições financeiras usuárias de serviços de Provedores de Serviços de Tecnologia da Informação (PSTI), conectados aos serviços de liquidação de transações do Sistema Financeiro Nacional (SFN).

2. ABRANGÊNCIA

Este plano aplica-se a todas as áreas internas da Cooperativa, vigorando por prazo indeterminado, devendo ser revisto periodicamente em função de sua efetividade na manutenção da continuidade dos negócios da Cooperativa.

3. DEFINIÇÃO E INDICAÇÃO DE PESSOAS ENVOLVIDAS

Todo processo crítico que envolva as rotinas essenciais para o correto e seguro andamento dos negócios da Cooperativa, deve ser devidamente mapeado por meio de levantamento de informações realizado pelo setor responsável pela Tecnologia da Informação (TI) da Cooperativa.

O presente Plano se caracteriza como um programa de administração de possíveis crises, o qual deve ser acionado sempre que identificados casos que provoquem a descontinuidade da oferta de produtos e serviços essenciais ao bom funcionamento da Cooperativa. Cabe ao setor de TI, sob supervisão das áreas de controle da Cooperativa, medir continuamente os impactos e a criticidade de eventos não esperados.

Tendo a disponibilidade de acesso e infraestrutura, deve-se efetuar uma varredura monitorada para auxiliar na identificação e extensão de possíveis problemas, executando as rotinas de teste básicos de conectividade e funcionalidades de sistemas.

Sendo detectado e confirmado um problema, o setor de TI deve manter a estrutura de atendimento aos associados e/ou clientes devidamente informados sobre possíveis interrupções de serviços.

Sempre que necessário, é responsabilidade do setor de TI entrar em contato com fornecedores para a solução de possíveis interrupções na prestação dos serviços contratados. Para tal o setor deve manter atualizada sua relação de contatos, com mais de um responsável disponível por prestador de serviços.

Havendo necessidade de contingenciamento, o setor deve adequar a comunicação interna do time de suporte e operações para auxiliar no atendimento aos associados e/ou clientes da Cooperativa, a fim de evitar transtornos ou realização de operações indevidas por meio dos seus canais de realização de transações.

Cabe ao setor de TI da Cooperativa coordenar as ações de sua estrutura própria, e/ou de seus fornecedores de serviços, no sentido de realizar com efetividade e registro adequado os seguintes procedimentos:

1. Avaliar os sistemas e recursos afetados;
2. Avaliar a adequação dos serviços prestados por fornecedores terceirizados;
3. Avaliar a sequência correta de procedimentos de responsabilidade de seus fornecedores;
4. Iniciar procedimentos de contingência;
5. Iniciar os procedimentos para reestabelecer os sistemas;
6. Definir procedimentos que serão necessários de acordo com processos de liberação;
7. Definir fornecedores que deverão ser acionados para reparo de infraestrutura;
8. Efetuar procedimentos de restauração de backup;
9. Definir com segurança a finalização da ocorrência e procedimentos para o retorno dos sistemas;
10. Elaborar relatórios com detalhes dos possíveis incidentes enfrentados;
11. Revisitar os eventos e todas as suas consequências a fim de avaliar se o plano de continuidade de negócios está adequado às exigências da Cooperativa e seus associados e/ou clientes.

4. PLANO DE CONTINGÊNCIA

Deve ser acionado sempre que as medidas de prevenção tenham falhado (redundância de links, discos, fornecimento elétricos e afins).

O plano de contingência deve ser elaborado para cada processo crítico que envolva o fornecimento de soluções tecnológicas utilizadas pela Cooperativa. Cabe ao setor de TI identificar os processos críticos que devam ser alvo de elaboração de seu respectivo plano de contingência.

A Cooperativa conta ambientes de redundância a fim de fornecer soluções para o correto funcionamento de sua capacidade principal de operação, bem como de sua capacidade de contingenciamento, permitindo a correta funcionalidade de seus produtos e serviços.

A infraestrutura de computação em nuvem da Cooperativa conta com a alta performance de entrega do ambiente AWS (*Amazon Web Services*), distribuídos estrategicamente em território nacional brasileiro.

5. DEFINIÇÃO DE DESASTRE

Será considerado desastre todo o incidente cujo tempo total de recuperação dos processos for superior a 60 minutos de entrega das soluções.

6. MONITORAMENTO

Todo colaborador da Cooperativa, ao constatar alguma anomalia que interfira na qualidade ou disponibilidade de qualquer processo sensível, deve comunicar ao setor responsável pelo acionamento dos planos de contingência, por meio dos canais internos disponíveis.

7. DECLARAÇÃO DE DESASTRE

Na ocorrência de qualquer evento que paralise algum processo essencial ao negócio da Cooperativa, cabe ao setor de TI, em conjunto com a área de negócios da Cooperativa, avaliar e relatar a ocorrência ao Diretor responsável.

Com base nas informações recebidas e avaliação do grau de impacto, compete ao Diretor decidir sobre a declaração da contingência.

8. SUPORTE E ATENDIMENTO AO CLIENTE

Cabe ao setor de negócios, em conjunto com o setor de comunicação elaborar mecanismos de comunicação com os associados e clientes, a fim de minimizar os transtornos provocados pela descontinuidade de serviços e produtos da Cooperativa.

9. PROCEDIMENTOS

Qualquer colaborador deverá estar apto a identificar, e reportar às alçadas competentes, toda e qualquer ameaça que possa levar à perda de qualidade e segurança, ou à descontinuidade dos negócios oferecidos pela Cooperativa.

10. RETORNO À NORMALIDADE

Cabe ao Diretor de Tecnologia da Informação encerrar o estado de contingência e comunicar aos Gestores envolvidos no processo.

11. ADMINISTRAÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS

A continuidade de negócios, assim como a recuperarão de desastres é o resultado da execução e da Manutenção de um processo contínuo de planejamento, formalização, monitoramento e ajustes contínuos.

A implantação do Plano de Continuidade de Negócios é de responsabilidade do Diretor Executivo responsável pela área de TI, que determina o ciclo e as etapas que deverão ser executadas para que, tanto os cenários de risco e impacto sobre os negócios, como as estruturas e estratégias que embasam o Plano possam ser atualizados de modo a refletir as necessidades e exigências normativas que regulam o SFN.

Para que a Diretoria possa verificar o grau de eficácia e atualidade do Plano de Continuidade de Negócios e decidir quanto ao momento em que o processo de continuidade de negócios deverá ser atualizado, serão consultados os setores responsáveis pelo planejamento de negócios e gerenciamento de riscos, de forma a estabelecer pontos de monitoramento para o setor de controles internos e conformidade (*compliance*) da Cooperativa.

12. TREINAMENTO

Um dos fatores primordiais para o funcionamento deste Plano é o conhecimento e a familiaridade das pessoas envolvidas na execução das atividades de continuidade de negócios e recuperação de desastres com as estratégias e recursos definidos no planejamento.

Para que seja possível esta familiaridade e conhecimento do plano, conferindo-lhe credibilidade, a equipe da Cooperativa deve tomar conhecimento do teor da Política de Segurança Cibernética, bem como os Planos dela decorrentes.

Para tal, a Cooperativa deve promover atividades semestrais de formação e divulgação do conteúdo do presente Plano, a fim de que todos os envolvidos tenham clareza do papel que devem desenvolver a fim de manter alto grau de continuidade dos negócios oferecidos aos associados e clientes.

Estas sessões serão organizadas pela área de TI, em conjunto com as áreas de negócios e de controles internos, com o objetivo de manter os colaboradores atualizados

sobre os conceitos de continuidade adotados, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação de desastres.

Para que este conhecimento seja preservado, os colaboradores admitidos e os transferidos para funções críticas de negócios, principalmente aqueles que pertencem à equipe de contingência, deverão ser instruídos das suas respectivas responsabilidades na aplicação do presente Plano de Continuidade de Negócios.

13. TESTES

Os testes têm por objetivo assegurar a eficiência e a efetividade do Plano de Continuidade de Negócios e deverão ser planejados e executados com periodicidade mínima anual a partir da data da sua implantação.

A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da área de TI.

Os cenários deverão ser definidos e registrados em documento formal devidamente aprovado pela alta administração da Cooperativa.

Os testes, sempre que possível, não deverão provocar qualquer tipo de indisponibilidade ou parada nos ambientes de negócios da Cooperativa e serão conduzidos pela equipe de contingência, em total conformidade com o definido nos cenários construídos. As simulações deverão ser realizadas sobre cenários e amagas contemplados no Plano, devendo cobrir os riscos e ameaças com maior probabilidade de ocorrência.

14. REDUNDÂNCIA ESTRUTURAL PARA FATORES CRÍTICOS EM NUVEM

Os sistemas de processamento da Cooperativa atuam hospedados de forma primária em um ambiente AWS *Cloud* e, de forma secundária, em um ambiente Microsoft Azure, aplicando-se a esses ambientes conexões em formato VPN com alto nível de criptografia.

Os *Backups* são feitos em outras estruturas de *Storage* com 3 replicações garantindo, assim que necessário, a atuação em um cenário de Recuperação de Desastre, temos também um ambiente físico controlado em nossa sede em Porto Alegre (RS).

15. REVISÃO

O presente Plano de Continuidade de Negócios é aprovado pela Diretoria Executiva da Cooperativa, devendo ser revisado semestralmente.

ANEXO II – PLANO DE RECUPERAÇÃO DE *BACKUP*

1. OBJETIVOS

O objetivo do presente Plano de Recuperação de *Backup*, parte anexa à sua Política de Segurança Cibernética, é divulgar as formas, procedimentos e métodos utilizados pela Cooperativa na execução das cópias de segurança (*backups*) de seus arquivos e documentos, deixando claras as definições técnicas, normas e responsabilidades, além de toda a metodologia de recuperação de dados e ativos.

2. DEFINIÇÕES

Para o que disposto no presente documento, considera-se:

a. ***Backup*:** toda e qualquer forma de cópia de segurança de dados computacionais, que pode ser consultada e/ou utilizada quando em momento posterior à sua restauração, em situações de indisponibilidade, alteração ou perda dos dados originais;

b. **Administrador de *backup*:** colaborador da Cooperativa, ou terceiro contratado para tal, responsável pelos procedimentos relacionados à configuração, execução, monitoramento e testes dos processos de *backup* e restauração de arquivos;

c. ***Full Backup* (Completo):** m*odalidade de backup onde todos os dados são armazenados.*

d. ***Backup* Diferencial:** modalidade de *backup* onde apenas os arquivos novos, ou aqueles modificados desde o último *full backup* (completo), são copiados;

e. ***Backup* Incremental:** modalidade de *backup* onde somente os arquivos novos ou modificados desde o último *backup*, independentemente de sua categoria, são copiados.

f. **Clientes de *backup*:** todo equipamento ou servidor onde é instalado o agente de *backup*;

g. **Recuperação de Desastre (Disaster Recovery):** planos de recuperação de dados motivados por situações de grave amplitude, seja ela física ou lógica;

h. **Unidade de armazenamento:** meio físico ou virtual onde os dados de um *backup* estão efetivamente armazenados;

i. **Retenção:** período em que o conteúdo da mídia de *backup* deve ser preservado e armazenado;

j. **Teste de restauração:** Procedimento amostral de teste de restauração. O teste deve ocorrer ao menos uma vez por ano com o intuito de garantir a efetividade do procedimento de *backup*;

k. ***Recovery Point Objective* - RPO:** momento em que os dados devem ser recuperados após situações de parada ou perda. Faz menção à quantidade máxima de tempo em que a Cooperativa consegue operar, apesar da perda de dados;

l. ***Recovery Time Objective* - RTO:** tempo estimado necessário para que se restaure os dados críticos que foram perdidos, e torne os serviços operantes novamente;

m. **Objeto:** qualquer dado que possa ser objeto de *backup* e/ou restauração.

3. RESPONSABILIDADES DO ADMINISTRADOR DE *BACKUP*

O Administrador de *backup* será responsável pela aplicação do presente Plano, bem como pelos procedimentos aqui estabelecidos, devendo organizar os serviços de *backup* e de restauração, além de gerir as unidades de armazenamento e assegurar o devido cumprimento de quaisquer normas aplicáveis.

Para tanto, consideram-se atribuições do Administrador de *backup*:

a. Propor modificações e melhorias à presente Política, visando o aperfeiçoamento das atividades despendidas;

b. Criar e gerir os *backups*, especialmente aplicando testes (inclusive de *restore*);

c. Configurar adequadamente as ferramentas e clientes de *backup*;

d. Criar e manter as unidades de armazenamento;

e. Delimitar quais objetos devem ser alvos de *backups* e restaurações;

f. Realizar teste de *backup* e *restore*;

g. Criar relatório e notificações, além de periodicamente verificar aqueles fornecidos pelas ferramentas de *backup*;

h. Em caso de necessidade, restaurar os *backups* existentes;

i. Prezar pela correta manutenção dos *backups* e seus dispositivos, realizando tratamento de quaisquer erros que possam surgir no transcorrer das operações;

j. Realizar o carregamento de unidades de armazenamento em locais de guarda apropriados;

k. Administrar os *logs* diários do *backup*;

l. Manter atualizado o inventário de *backup.*

4. *BACKUP* E SUA ATUALIZAÇÃO

Para realização de *backups* e devido cumprimento das obrigações apontadas, deve-se considerar e avaliar toda e qualquer unidade de armazenamento que esteja sob responsabilidade da Cooperativa ou fornecedor terceirizado.

As cópias de segurança dos *backups* devem ser protegidas por metodologias capazes de garantir a restrição de acesso, além de questões como confidencialidade, integridade e disponibilidade das informações armazenadas.

A avaliação e decisão de quais arquivos serão incluídos no *backup* será responsabilidade do Administrador de *backup* da Cooperativa, sob supervisão da Diretoria responsável pela área de TI, o qual terá como prioridade a inclusão de arquivos de configurações e sistemas operacionais e aplicativos instalados nos servidores, configuração do banco de dados, documentos e e-mails por usuário e arquivos de log dos aplicativos, incluindo-se o *log* do *backup* e *restore*.

Os *backups*, independentemente de sua categoria, serão realizados quando novas aplicações forem desenvolvidas, novas unidades de armazenamento forem adquiridas ou utilizadas, e quaisquer outros objetos sejam apresentados aos sistemas da Cooperativa.

Todo e qualquer item que necessite de proteção e retenção será informado ao Administrador de *backup*.

5. RETENÇÕES, CRIAÇÃO E OPERAÇÃO DOS BACKUPS

Os *backups* terão sua retenção de acordo com os seguintes prazos:

b. Diário: 30 dias.
c. Semanal: Entre 4 e 6 últimas semanas.
d. Mensal: De 6 a 12 meses.
e. Anual (Entire System): 13 meses

Deve-se programar a realização dos *backups* de modo a gerar o menor impacto possível na produção, em momentos de pouca utilização da rede e dos sistemas da Cooperativa, antes ou após os horários de operação e principalmente dos horários de pico produtivos da empresa, recomendando-se que:

***Backups* Diários**	De segunda a sexta-feira, às 22:00 horas.
***Backups* Semanais**	Aos finais de semana.
***Backups* Mensais**	No primeiro sábado do mês.

O procedimento relacionado à realização dos *backups* será monitorado pelo Administrador de *backup*, o qual também analisará os relatórios de acompanhamento de *backup* gerados pelo sistema, seja em relação aos *backups* realizados com sucesso bem como acerca de possíveis falhas e erros. Em sendo apresentadas falhas, ao Administrador de *backup* competirá a adoção de medidas corretivas.

Expirado o referido prazo de retenção, as Unidades de Armazenamento poderão ser destruídas ou reutilizadas, considerando sempre seu estado de conservação e utilização, mediante decisão fundamentada pelo Administrador de *backup*, aprovada pelo Diretor responsável pelo pela TI da Cooperativa.

6. *RESTORE* E SEUS PROCEDIMENTOS

A Recuperação de Desastre (*Restore*) será de responsabilidade do Administrador de *backup*, podendo ser requisitada por qualquer colaborador que dela dependa, desde que através de pedido por escrito, capaz de identificar o solicitante, ainda que por meio eletrônico, devidamente motivado.

Na referida solicitação devem constar quais Objetos, Clientes de Backups, Unidades de Armazenamento, bem como demais informações necessárias para que se localize e identifique o que desejado.

Após o *Restore*, o Administrador de *backup* emitirá relatório sobre o procedimento, apontando qualquer erro ou falhas que ocorram em todo o processo. O tempo do *Restore* não pode passar de 8 horas, delimitando-se assim o *RTO*, para que os serviços e operações da Cooperativa não sejam significativamente afetados.

Da mesma forma que os *backups*, os procedimentos de *Restore* deverão ser testados de forma semestral ou anual, sendo anotados em relatórios emitidos pelo Administrador de *backups* quaisquer erros metodológicos ou vinculados aos programas e meios utilizados.

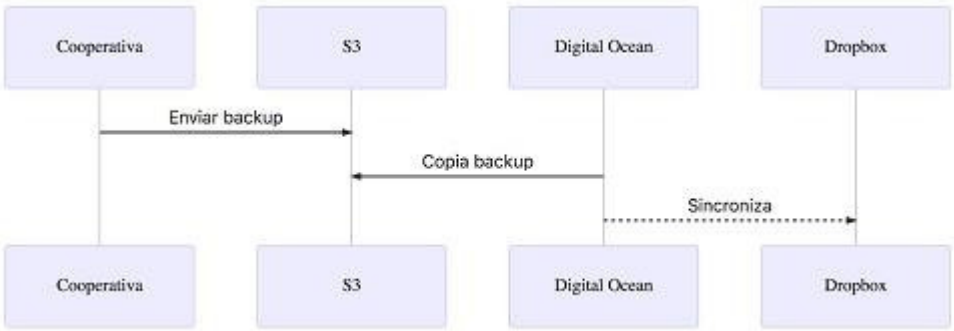
7. NÍVEIS DE REDUNDÂNCIA

Nos processos de *backup* executados pela Cooperativa, são utilizados 3 níveis de redundância de dados com o intuito de obter maior resiliência e segurança.

Inicialmente, os dados são copiados para um servidor de armazenamento local. Posteriormente, uma segunda cópia dos dados, é enviada para um serviço externo de armazenamento de dados em nuvem. Finalmente, uma terceira cópia dos dados é enviada para outro serviço externo de armazenamento de dados em nuvem.

Utilizando-se dessa estrutura de replicação de dados em 3 camadas, é possível obter maior garantia de posse dos dados e segurança.

Abaixo um diagrama do processo de *backup* implementado para nossos clientes:



8. DISPOSIÇÕES FINAIS

O presente Plano de Recuperação de *Backup* é aprovado pela Diretoria Executiva da Cooperativa e deverá ser revisado anualmente, podendo sofrer correções e modificações, conforme relatórios emitidos pelo Administrador de *backup*, ou de acordo com as necessidades da Cooperativa.

ANEXO III – PLANO DE RESPOSTA A INCIDENTES

1. OBJETIVOS

O objetivo deste Plano de Respostas a Incidentes é descrever os processos e procedimentos que visam gerenciar, controlar e reportar os dados relacionados a Incidentes de Segurança, os quais podem ter suas origens em fontes internas ou externas de processamento de informações sensíveis da Cooperativa e partes relacionadas.

Visa também o presente plano a estabelecer procedimentos para comunicação de vulnerabilidades na segurança de informação por agentes internos ou externos.

Importante que os registros de incidentes de Segurança da Informação, bem como vulnerabilidades reportadas, sejam devidamente monitorados, investigados e gerenciados, de modo a tomar as devidas providências imediatas de resolução, bem como a implantação de medidas que visem diminuir o risco de repetição futura dos mesmos.

Em determinadas circunstâncias, seguindo o arcabouço legal e normativo, se fará necessária a comunicação dos incidentes às autoridades relacionadas, bem como aos demais instituições participantes do Sistema Financeiro Nacional (SFN).

2. ESCOPO

As diretrizes descritas neste Plano têm como finalidade padronizar as ações referentes às áreas de processos previstos na Política de Segurança Cibernética da Cooperativa, organizando infraestrutura e equipe para a adequada resposta a incidentes de segurança da informação, definindo as atividades que deverão ser executadas, tempestivamente, pelos responsáveis.

3. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Considera-se incidente de segurança da informação, para efeito deste Plano, todo e qualquer evento ou situação associada aos serviços de Tecnologia da Informação (TI) que:

1. possa expor a organização ou seus sistemas, a cenários de ameaças contra a integridade, confidencialidade e disponibilidade das informações em posse e/ou responsabilidade da Cooperativa.

2. possa resultar em perdas, danos aos ativos de Tecnologia da Informação da Cooperativa;

3. viole, acidentalmente ou intencionalmente, as normas previstas na Política de Segurança Cibernética da Cooperativa, bem como no arcabouço legal ou normativo vigente.

4. DESCRIÇÃO E TIPOS E INCIDENTES

Nº	Tipo	Descrição	Baixa Confidencialidade Assegurar que a informação apenas está acessível a quem está autorizado	Média Integridade Salvaguardar que a informação e o método de processamento são exatos e completos	Alta Disponibilidade Assegurar que os utilizadores autorizados têm acesso à informação quando necessário
1	Incidente Malicioso	Qualquer ação intencional que leve a perda, dano ou corrupção dos ativos de TI	Acesso não autorizado à informação tem um efeito adverso limitado nas operações	O acesso não autorizado à informação tem um efeito significativo nas operações	O acesso não autorizado à informação tem um efeito adverso catastrófico nas operações
2	Violação de Acesso	Uso não autorizado de sistema de TI, incluindo mau uso de contas e senhas			
3	Furto/Roubo	Roubo ou furto de qualquer equipamento de TI	Uma alteração não autorizada à informação ou destruição da mesma tem um efeito adverso e limitado nas operações	Uma alteração não autorizada à informação ou destruição tem um efeito significativo nas operações	Uma alteração não autorizada a informação ou destruição tem um efeito catastrófico nas operações
4	Uso Inadequado	Mau uso de facilidades para acessar conteúdo			
5	Acidente	Qualquer falha acidental ou não intencional	O não acesso ou impossibilidade de utilização da informação ou sistemas tem um efeito limitado nas operações	O não acesso ou impossibilidade de utilização da informação ou sistemas tem um efeito significativo nas operações	O não acesso ou impossibilidade de utilização informação ou sistemas tem um efeito catastrófico nas operações
6	Incidente Operacional	Evento de falha de sistema ou mudança em uma configuração que resulte em perdas de disponibilidade ou integridade de sistemas			

5. PRIORIZAÇÃO

Os incidentes devem ser priorizados conforme tabela abaixo:

Nível Prioridade	Descrição Prioridade	Observação	Resposta
Baixa	Um evento de baixo impacto com pouco ou nenhum efeito operacional e que requer pouco esforço para gerenciar e resolver.	Incidente de vírus em um único computador ou dispositivo. Diversas tentativas malsucedidas de obter acesso não autorizado.	Resolvido por agentes da equipe de resposta com ações já mapeadas.
Média	Possível brecha de segurança que requer investigação e envolvimento do Comitê de Segurança e Privacidade da Informação para resolução.	Acesso não autorizado a uma conta de serviço. Tentativa de acesso à sala de servidores. Escaneamento de portas em rede interna ou externa. Múltiplos incidentes de vírus.	Precisa ser escalado para o Comitê de Segurança e Privacidade da Informação para coordenação, investigação e resolução.
Alta	Evento com impacto significante a serviços críticos de TI ou informações, dano a equipamento físico ou a pessoas	Violação em larga escala de dados sensíveis a pesquisa, dados financeiros ou pessoais. Pichação do website da instituição. Acesso não autorizado à sala de servidores.	Precisar ser escalado ao Gerente de Tecnologia da Informação e ao Comitê de Segurança e Privacidade da Informação Imediatamente. Todos os envolvidos precisam ser notificados.

6. NOTIFICAÇÕES

Todos os incidentes devem ser notificados por qualquer usuário interno ou externo, como associados, clientes, parceiros, fornecedores e colaboradores, por meio dos canais disponibilizados internamente ou intranet.

Os canais devem ser divulgados internamente para facilitar o registro de atividades suspeitas e/ou incidentes identificados.

7. EVIDÊNCIAS E ARMAZENAMENTO

De acordo com o tratamento das atividades referente a incidentes todas as evidências devem ser coletadas e armazenadas, bem como, todas as ações devem ter seus registros através de solução de suporte permitindo a correta análise por parte de autoridades e pessoas autorizadas.

Toda evidência deve comtemplar o seguinte pacote de informações:

1. Logs de auditoria [*Firewall*, Banco de Dados, *Proxys*, Estação e Servidor);
2. Arquivos *Malware*;
3. Dumps de memória da estação ou servidor afetado;
4. Dados de e-mails;
5. Alertas de Segurança;
6. Dados, históricos, *logs* e *Changes Requests* sobre os sistemas comprometidos;
7. Imagem de disco virtual.

Todos os incidentes devem ser documentados na ferramenta de registro de incidentes disponibilizado pela área de TI da Cooperativa, respeitando as informações abaixo como obrigatórias:

1. Todas as informações dadas como breve relato pelo usuário;
2. Ações identificadas pelo time de suporte, operações e infraestrutura;
3. Diagnóstico referente aos processos de investigações;
4. Toda informação de contato.

Durante o tratamento de qualquer incidente, os usuários não devem realizar qualquer tipo de alteração, modificação ou qualquer tipo de interferência nos sistemas comprometidos até que a equipe responsável pela resposta autorize.

8. LISTA DE VERIFICAÇÃO AO CORRETO TRATAMENTO DE INCIDENTES

Ações para o tratamento de incidentes de Segurança da Informação		
	Ação	**Responsável**
1	**Procedimento para tratamento de notificação de incidente** - Reporte deve ser recebido via e-mail ou mecanismo de comunicação devidamente institucionalizado pela Cooperativa; - Todos os detalhes precisam ser registrados, incluindo detalhes de contato, e o registro deve ser atribuído para um membro da equipe de resposta.	Equipe de resposta a incidentes de segurança da informação
2	**Revisar detalhes e atribuir prioridade** - O incidente deve ser atribuído a um membro da equipe de resposta a incidente e deve ser tratado com uma solução já mapeada.	Equipe de resposta a incidentes de segurança da informação

Ações para o tratamento de incidentes de prioridade baixa		
	Ação	**Responsável**
1	**Contenção ou remoção de ameaça** - O incidente deve ser atribuído a um membro da equipe de resposta a incidente e deve ser tratado com uma solução já mapeada; - O membro responsável deve seguir a orientação descrita em roteiros já mapeados; - As ações podem conter a remoção de vírus, *reset* de conta de usuário ou ainda o contato direto com o usuário impactado; - Se um computador contiver um vírus de baixo impacto, o dispositivo deve ser desconectado da rede para prevenir a propagação. Outros computadores devem ser analisados para verificação de comprometimento.	Equipe de resposta a incidentes de segurança da informação
2	**Recuperação/restauração dos sistemas afetados** - Uma vez que a causa do incidente foi solucionada, o computador ou a conta de usuário deve ser recuperada; - Em eventos em que há comprometimento de sistemas, como numa infecção de vírus ou outra vulnerabilidade, o sistema operacional deve ser reinstalado para remover todos os traços da infecção. Após este processo, a máquina pode ser reconectada à rede.	Equipe de resposta a incidentes de segurança da informação

3	**Documentação dos resultados** - Toda a investigação e as ações de recuperação precisam ser registradas no sistema de registro de incidentes; - Todos os detalhes relacionados com a resolução do incidente deve ser anotado de forma clara e detalhada .	Equipe de resposta a incidentes de segurança da informação

Ações para o tratamento de incidentes de prioridade média		
	Ação	**Responsável**
	Investigação Inicial O Comitê de Segurança e Privacidade da Informação precisa revisar um incidente antes de ser considerado médio ou alto, a fim de validar as informações e definir quais os passos para iniciar a investigação. Os seguintes fatores precisam ser considerados ao elevar a prioridade de um incidente para Alta: - Dados pessoais ou privados foram comprometidos? - O impacto é visivelmente público? - O incidente pode impactar negativamente a reputação da Cooperativa ou seus produtos e serviços?	Equipe de resposta a incidentes de segurança da informação
2	**Contenção ou remoção de ameaça** - Os incidentes devem ser atribuídos a um membro do Comitê de Segurança que pode acionar qualquer outro funcionário, caso necessário; - O comitê precisa determinar se algum computador será confiscado até que a investigação seja realizada. Em algumas circunstâncias, o computador precisa ser desligado da rede até que se tenha um parecer favorável ao restabelecimento pela equipe técnica; - Todos os vírus, material impróprio ou outras causas de um incidente devem ser removidos durante a contenção para prevenir a propagação ou o comprometimento de outros sistemas.	Equipe de resposta a incidentes de segurança da informação
3	**Remediar vulnerabilidades identificadas** - A investigação de um incidente pode revelar fraquezas ou vulnerabilidades nos processos de controle de segurança; - O comitê deve identificar, documentar e tomar ação para remediar as fraquezas e as vulnerabilidades implementando ou adaptando controles para prevenir a repetição do evento; - A remediação pode se estender para análise de violações a políticas de segurança e, nestes casos, o Comitê deve prover a conscientização ao usuário envolvido.	Equipe de resposta a incidentes de segurança da informação

4	**Recuperação/restauração dos sistemas afetados** - Uma vez que a causa do incidente foi solucionada, o computador ou a conta de usuário deve ser recuperada; - O objetivo desta recuperação é restabelecer os sistemas afetados de forma a evitar futuros incidentes semelhantes; - O comitê definirá se o sistema operacional deve ser reinstalado ou um backup disponibilizado para permitir a recuperação; - Uma vez que isto ocorra, o sistema pode ser reconectado à rede, para retorno a suas atividades normais.	Equipe de resposta a incidentes de segurança da informação
5	**Condução de revisão e relatório pós-incidente** - O comitê deverá rever a documentação e as evidências coletadas para determinar a causa raiz além de prover recomendações para prevenir a recorrência deste incidente; - Recomendações levantadas devem ser entregues em relatório pós-incidente para o Gerente de Tecnologia da Informação; - O comitê deve informar os usuários impactados diretamente e os que reportaram problema inicial.	Equipe de resposta a incidentes de segurança da informação

Ações para o tratamento de incidentes de prioridade alta		
Ação		**Responsável**
1	**Investigação Inicial** O Comitê de Segurança e Privacidade da Informação precisa revisar um incidente antes de ser considerado médio ou alto, a fim de validar as informações e definir quais os passos para iniciar a investigação. Os seguintes fatores precisam ser considerados ao elevar a prioridade de um incidente para Alta: - Dados pessoais ou privados foram comprometidos? - O impacto é visivelmente público? - O incidente pode impactar negativamente a reputação da Cooperativa ou seus produtos e serviços?	Equipe de resposta a incidentes de segurança da informação

	Acionamento do Time de Resposta a incidentes Dado o tamanho de um incidente de alta prioridade, o Gerente de Tecnologia da Informação será responsável por acionar e coordenar os trabalhos dos especialistas necessários. Isto irá permitir a coordenação centralizada das ações para resposta ao incidente com o intuito de evitar impacto negativo à instituição. A comunicação entre os envolvidos é fundamental para permitir a rápida resposta. A força tarefa pode ser dividida em três frentes: - Investigação: Identificar a causa, motivação, usuários envolvidos e o dano causado pelo incidente; - Contenção: Implementação de ações de monitoração e de controles de correção para reduzir o impacto durante um incidente; - Restauração: Recuperação dos sistemas impactados ou ativação de plano de recuperação de desastres para restaurar os serviços para um estado seguro.	Gerente de Tecnologia da Informação
3	**Notificar envolvidos relevantes** Em eventos de alta prioridade, o Gerente de Tecnologia da Informação irá determinar quem precisa ser notificado do incidente: - O mantenedor da instituição; - Funcionários e clientes; - Agências do governo; - Empresas parceiras; - Comunidade.	Gerente de Tecnologia da Informação
4	**Condução de revisão e relatório pós-incidente** - O Gerente de Tecnologia da Informação deverá conduzir um processo formal de revisão do ocorrido apresentando uma breve discussão sobre a causa raiz do incidente, provendo feedback sobre a resposta dada para resolução do problema e sobre as recomendações de melhoria.	Gerente de Tecnologia da Informação
5	**Revisão dos resultados** O Gerente de Tecnologia da Informação deve promover ações de melhoria para que novos incidentes sejam evitados. O Gerente de Tecnologia da Informação deve avaliar todo o processo de tratamento em busca do aperfeiçoamento das ações tomadas para contenção e erradicação do incidente.	Gerente de Tecnologia da Informação

9. PAPÉIS E RESPONSABILIDADES

Para a execução das atividades deverá promover recursos e estrutura necessários, contemplando recursos humanos e financeiros, bem como infraestrutura e treinamentos em processos e ferramentas requeridas para a sua correta execução.

a. Comitê de Tecnologia de Informação

Cabe ao Comitê de Tecnologia de Informação:

1. Analisar todos os registros relevantes;
2. Elaborar relatório periódico de auditoria;
3. Analisar ações de acordo com incidentes e suas corretas identificações que possam representar vulnerabilidades na segurança;
4. Garantir que ações de melhoria tenham seus devidos impactos e recomendações implementadas;
5. Conduzir revisões pós incidentes e resoluções implantadas;
6. Comunicar o processo de cada resposta aos incidentes identificados aos envolvidos;
7. Apresentar indicadores pós incidentes;

b. Diretor de Tecnologia da Informação

Deve aprovar o envolvimento correto dos recursos internos e externos, durante a atividade de resolução, análise de incidentes críticos.

Aprovar adequadamente a comunicação interna relevantes e notificar as camadas de lideranças internas e externas quanto a identificação e resolução se necessário.

c. Equipe de tratamento a incidentes de segurança e respostas

Promover suporte e orientação para detectar e resolver incidentes de segurança da informação de acordo com o item 3 deste Plano.

Reportar incidentes e vulnerabilidades conhecidas ao comitê interno de segurança e riscos se necessário.

Execução de ações corretivas para resolução de incidentes quanto a segurança da informação.

10. COMUNICAÇÃO AOS ENVOLVIDOS

Conforme a resposta a incidentes tem seu desfecho adequado, todos os envolvidos devem ser comunicados sobre o andamento e a resolução do incidente e resposta.

Em tempo de análise e resolução todas as informações devem ser mantidas em confidencialidade.

Quando de um incidente de alta prioridade e impacto deve ser avaliada a necessidade de comunicação às autoridades competentes, órgãos de supervisão e demais instituições atuantes no Sistema Financeiro Nacional.

O presente Plano de Respostas a Incidentes é aprovado pela Diretoria Executiva da Cooperativa e deve ser revisado semestralmente, a fim de avaliar sua efetividade.