Uniprime cooperativa de crédito	**PLANO DE AÇÃO E DE RESPOSTAS A INCIDENTES DE SEGURANÇA CIBERNÉTICA**		
Elaborado por: Uniprime Greencred			Data da Criação: 12/08/2026
Aprovador por: Conselho de Administração		Ata n.º **008/26**	Data Aprovação: 17/08/2026
Início da vigência: 17/08/2026	Revisado em:		

Sumário

1 OBJETIVO

O presente Plano de Ação e de Resposta a Incidentes (“Plano”) tem por objetivo estabelecer diretrizes, responsabilidades e fluxos para prevenção, detecção, registro, tratamento, resposta, comunicação e recuperação de incidentes de segurança no âmbito da Uniprime Greencred, em observância à Política de Segurança Cibernética e à regulamentação aplicável.

O Plano visa assegurar a adequada gestão dos incidentes, bem como estabelecer mecanismos de escalonamento e avaliação de sua relevância para fins regulatórios, operacionais e de continuidade de negócios.

2 REFERÊNCIAS NORMATIVAS

Este Plano observa a legislação, regulamentação, normativos internos aplicáveis, especialmente:

- Política de Segurança Cibernética;
- Plano de Continuidade de Negócios;
- Resolução CMN nº 4.893/2021;
- Resolução CMN 5274/2025;
- Resolução BCB nº 01/2020, incluindo regras dos Manuais do Pix;
- Instrução Normativa BCB n° 412/2023;
- Lei nº 13.709/2018; e
- Resolução CD/ANPD nº 15/2024.

3 ABRANGÊNCIA

O presente Plano de Ação e Resposta a Incidentes aplica-se à Uniprime Greencred.

4 DEFINIÇÕES

Colaboradores: conjunto de pessoas que atuam em nome da cooperativa, incluindo empregados, membros da diretoria, estagiários, jovens aprendizes, prestadores de serviços e quaisquer outros prepostos.

Uniprime Greencred: cooperativa singular filiada ao Sistema Uniprime.

Corrupção de Dados: alteração, degradação, perda de integridade ou inconsistência de dados armazenados ou em processamento, decorrente de ação não autorizada, falha técnica, operacional ou de segurança, que comprometa sua confiabilidade ou utilização adequada.

Credenciais Privilegiadas: credenciais de autenticação associadas a acessos administrativos capazes de conceder poderes de administração, gerenciamento, configuração ou controle sobre sistemas, ambientes, Processos Críticos, serviços ou ambientes mantidos por Fornecedores Relevantes relacionados à cooperativa.

Fornecedor Relevante: fornecedor ou prestador de serviços, cuja relação comercial possa impactar significativamente a continuidade operacional, a conformidade regulatória, a segurança da informação, a situação financeira, a reputação ou a prestação de serviços essenciais da cooperativa, em razão da criticidade do serviço prestado, do volume financeiro envolvido, do acesso a dados/informações sensíveis ou da dependência operacional existente.

Grupo de Trabalho: grupo multidisciplinar responsável pela condução das atividades relacionadas ao Ciclo de Resposta a Incidentes, composto, conforme a natureza e a criticidade do Incidente de Segurança, por representantes das áreas de Segurança Cibernética, Tecnologia da Informação, Compliance, Jurídico, Encarregado pelo Tratamento de Dados Pessoais (“Encarregado”) quando houve o envolvimento de dados pessoais, Diretor responsável pelo Pix quando houver impactos no Pix, gestores de áreas impactadas e, quando aplicável, Comunicação.

Incidente de Segurança: um evento que coloca em risco a confidencialidade, integridade, disponibilidade e/ou autenticidade de um sistema de informação ou de dados que o sistema processa, armazena ou transmite, ou que constitui uma violação ou ameaça iminente de violação das políticas ou procedimentos de segurança. Uma "ameaça iminente de violação" se refere a uma situação em que a organização tem uma base factual para acreditar que um incidente específico está prestes a ocorrer.

Indisponibilidade parcial de sistemas: evento que resulte na limitação, degradação ou indisponibilidade parcial de sistemas, aplicações, ambientes ou recursos tecnológicos utilizados pela cooperativa, reduzindo sua capacidade operacional ou desempenho esperado, sem ocasionar interrupção total dos serviços financeiros ou de pagamentos.

Interrupção parcial de serviços financeiros ou de pagamentos: evento que resulte na degradação, limitação ou indisponibilidade parcial de serviços financeiros, serviços de pagamento, sistemas ou processos críticos relacionados à sua prestação, reduzindo sua capacidade operacional, desempenho ou disponibilidade, sem impedir integralmente sua execução, podendo demandar a adoção de medidas de contingência para manutenção do nível mínimo operacional definido pela Uniprime Greencred.

Interrupção total de serviços financeiros ou de pagamentos: evento que resulte na indisponibilidade completa de serviços financeiros, serviços de pagamento, sistemas ou processos críticos relacionados à sua prestação, impedindo integralmente a execução das atividades a eles associadas dentro dos níveis mínimos aceitáveis definidos pela Uniprime Greencred, demandando a avaliação da aplicação das medidas de contingência e recuperação previstas no Plano de Continuidade de Negócios (“PCN”).

Malware: um trojan, vírus, worm ou qualquer outro software malicioso que pode prejudicar sistemas, serviços ou redes, impactando as informações ali contidas.

Negação de Serviço (DoS) e Negação de Serviço Distribuída (DDoS): sobrecarga um serviço com tráfego, impactando a disponibilidade informações.
Phishing: mensagens enganosas projetadas para obter dados confidenciais dos usuários (como logins bancários ou credenciais de login de negócios) ou usadas para executar código malicioso para permitir acesso remoto.

Processos Críticos: processo cuja interrupção, falha ou indisponibilidade, após avaliação com base nos critérios de impacto definidos no Plano de Continuidade de Negócios, seja classificada como capaz de gerar impactos relevantes sob a perspectiva financeira, operacional, legal/regulatória e reputacional, devendo, em razão dessa classificação, ser priorizado nas estratégias de continuidade e recuperação.

Ransomware: tipo de software malicioso (malware) destinado a bloquear, restringir ou inviabilizar o acesso a sistemas, dispositivos ou dados, geralmente por meio de criptografia, com exigência de pagamento de resgate para restabelecimento do acesso.

Serviço Relevante: qualquer serviço cuja interrupção, indisponibilidade, falha ou comprometimento de segurança possa impactar significativamente a continuidade das operações do Sistema, o cumprimento de suas obrigações legais e regulatórias, a proteção de dados e informações, a segurança das transações, a confiança de cooperados, ou que cause prejuízos financeiros e/ou reputacionais.

Sistema Uniprime: conjunto formado pela Uniprime Central Nacional e pelas Cooperativas Filiadas e não filiadas que a integram, atuando de forma coordenada na prestação de serviços financeiros e no atendimento aos cooperados.

Uniprime Central Nacional ou Uniprime: Cooperativa de crédito de segundo grau, responsável por organizar, coordenar e prover serviços às cooperativas Singulares integrantes do Sistema Uniprime.

Vazamento de Dados: acesso não autorizado que resulta em divulgação de dados, que comprometem a confidencialidade das informações.

Vulnerabilidade: uma fraqueza (ou falha) em um sistema, nos procedimentos de segurança do sistema, nos controles internos ou na implementação, pela qual um agente ou evento pode explorar intencionalmente ou acionar acidentalmente a vulnerabilidade para acessar, modificar ou interromper as operações normais de um sistema, resultando em um incidente de segurança ou na violação da política de segurança do sistema.

4.1 Vetores de Ameaça Comuns

Os vetores de ameaça são as vias pelas quais agentes maliciosos podem explorar vulnerabilidades e comprometer a segurança da informação da organização. Os vetores mais comuns incluem:

Atrito: um ataque que emprega métodos de força bruta para comprometer, degradar ou destruir sistemas, serviços ou redes (por exemplo, um ataque de Negação de Serviço com o intuito de prejudicar ou negar acesso a um serviço ou aplicativo; ou um ataque de força bruta contra um mecanismo de autenticação, como senhas ou assinaturas digitais).

E-mail: um ataque executado por meio de uma mensagem de e-mail ou anexo (por exemplo, código malicioso disfarçado como um documento anexado ou um link para um site malicioso no corpo de uma mensagem de e-mail).

Mídia Externa/Removível: um ataque executado a partir de mídia removível ou um dispositivo periférico (por exemplo, código malicioso se espalhando para um sistema a partir de mídia removível infectada).

Imitação: um ataque que envolve a substituição de algo benigno por algo malicioso (por exemplo, *spoofing*, ataques *man-in-the-middle*, pontos de acesso sem fio e ataques de injeção de SQL).

Uso indevido: qualquer evento resultante da violação das políticas de uso aceitável de uma organização por um usuário autorizado (por exemplo, um usuário instala um software de compartilhamento de arquivos, levando à perda de dados confidenciais; ou um usuário realiza atividades ilegais em um sistema).

Perda ou roubo de equipamento: a perda ou roubo de um dispositivo de computação ou mídia usada por uma organização, como um laptop, smartphone ou token de autenticação.

Web: um ataque executado a partir de um site ou aplicativo baseado na web (por exemplo, um ataque de script entre sites usado para roubar credenciais ou redirecionar para um site que explora uma vulnerabilidade do navegador da web e instala malware).

Falhas de hardware ou software: problemas técnicos que expõem os sistemas a vulnerabilidades ou falhas de segurança (por exemplo, não aplicação de um patch de segurança ou utilização de um equipamento infectado).

5 PAPÉIS E RESPONSABILIDADES

A Uniprime Greencred mantém estrutura de governança de segurança cibernética compatível com seu porte, perfil de risco, modelo de negócio e natureza das operações realizadas, assegurando a definição clara de papéis e responsabilidades para prevenção, tratamento, resposta e comunicação de Incidentes de Segurança.

5.1 Conselho de Administração

Compete ao Conselho de Administração:

I. Aprovar e revisar este Plano e suas respectivas atualizações no mínimo anualmente;
II. Supervisionar a efetividade da estrutura de resposta a incidentes; e
III. Tomar ciência dos incidentes relevantes e das medidas adotadas para mitigação de impactos e prevenção de recorrências.

Na inexistência de constituição de Conselho de Administração, aplicam-se à diretoria as responsabilidades a ele atribuídas por esta política.

5.2 Diretor Responsável pela Segurança Cibernética

Compete ao Diretor Responsável pela Segurança Cibernética:

IV. Determinar o acionamento deste Plano e definir a composição do Grupo de Trabalho, conforme a natureza, extensão e criticidade do Incidente de Segurança;
V. Coordenar as ações de resposta, contenção, erradicação e recuperação relacionadas ao Incidente de Segurança;
VI. Definir prioridades, prazos e direcionamentos para atuação das áreas envolvidas;
VII. Aprovar, quando necessário, o acionamento de terceiros especializados para apoio técnico, forense, operacional ou jurídico;
VIII. Atuar como ponto focal para alinhamento entre o Grupo de Trabalho, a alta administração e as áreas impactadas;
IX. Receber, coordenar e acompanhar demandas, questionamentos, ofícios e demais comunicações encaminhadas pelo Banco Central do Brasil relacionadas a Incidentes de Segurança;
X. Supervisionar, com apoio das áreas responsáveis, as comunicações regulatórias e institucionais decorrentes do Incidente de Segurança; e
XI. Reportar ao Conselho de Administração os incidentes relevantes e as medidas adotadas.

5.3 Diretor Responsável pelo Pix

Compete ao Diretor Responsável pelo Pix:

I. Apoiar a avaliação dos incidentes que afetem ou possam afetar o arranjo Pix;
II. Participar do Grupo de Trabalho nos incidentes relacionados ao Pix;
III. Conduzir, com apoio das áreas de Compliance e Jurídico, as comunicações regulatórias ao Banco Central do Brasil relacionadas ao Pix; e
IV. Acompanhar determinações, questionamentos, ofícios e demais comunicações encaminhadas pelo Banco Central do Brasil no âmbito do arranjo Pix relacionadas a Incidentes de Segurança.

5.4 Grupo de Trabalho

Compete ao Grupo de Trabalho:

I. Identificar, registrar, analisar e classificar os Incidentes de Segurança;
II. Levantar, preservar e documentar evidências relacionadas ao Incidente de Segurança;
III. Executar as medidas necessárias para contenção, erradicação e recuperação dos ambientes afetados;
IV. Avaliar os impactos operacionais, tecnológicos, regulatórios e reputacionais decorrentes do Incidente de Segurança;
V. Estabelecer prioridades de tratamento em casos de Incidentes de Segurança simultâneos;
VI. Manter registro formal das ações executadas e das decisões adotadas ao longo do ciclo de resposta; e
VII. Propor medidas corretivas, preventivas e melhorias de controles após a conclusão do tratamento do Incidente de Segurança.

5.5 Gestores das Áreas Impactadas

Compete aos Gestores das Áreas Impactadas:

I. Fornecer ao Grupo de Trabalho as informações necessárias para avaliação e tratamento do Incidente de Segurança;

II. Apoiar a identificação dos impactos operacionais e de negócio decorrentes do Incidente de Segurança; e

III. Colaborar com a implementação das medidas de contingência e recuperação aplicáveis.

5.6 Responsável Técnico pela Tecnologia

I. Comunicar a área de Segurança Cibernética da Uniprime Central Nacional qualquer indício, suspeita ou confirmação de incidente de segurança;

II. Identificar, registrar, classificar, analisar e apoiar o tratamento dos incidentes de segurança da informação e segurança cibernética;

III. Adotar medidas de contenção, mitigação, erradicação e recuperação dos ambientes e serviços afetados;

IV. Atuar na preservação de evidências técnicas e registros necessários à análise dos incidentes;

V. Apoiar a avaliação dos impactos operacionais, tecnológicos e de segurança decorrentes do incidente;

VI. Executar ou acompanhar a implementação das ações corretivas e preventivas definidas para mitigação de vulnerabilidades e redução de riscos;

VII. Apoiar na comunicação tempestiva dos incidentes às áreas responsáveis, observados os fluxos de escalonamento e reporte estabelecidos neste Plano;

VIII. Apoiar a realização de testes, simulações e exercícios relacionados à continuidade de negócios e resposta a incidentes;

IX. Atuar como ponto focal na atuação conjunta com a Uniprime Central Nacional, na contenção e tratamento dos incidentes.

5.7 Área Controles Internos

Compete à área de Compliance:

I. Apoiar a classificação regulatória do incidente, inclusive quanto à sua relevância;

II. Identificar obrigações regulatórias de comunicação e reporte aplicáveis;

III. Apoiar a elaboração e acompanhamento das comunicações ao Banco Central do Brasil e demais autoridades competentes junto à Uniprime Central Nacional, quando aplicável;

IV. Acompanhar a aderência das ações adotadas às políticas internas e à regulamentação vigente;

V. Manter os registros regulatórios relacionados ao Incidente de Segurança, quando aplicável;

VI. Acompanhar e manter registros dos testes, simulações e exercícios relacionados à continuidade de negócios e resposta a incidentes;

VII. Acompanhar a implementação das ações corretivas e preventivas definidas para mitigação de vulnerabilidades e redução de riscos.

5.8 Jurídico

Compete à área Jurídica:

I. Avaliar os impactos jurídicos decorrentes do Incidente de Segurança;

II. Apoiar a análise de obrigações contratuais relacionadas ao Incidente de Segurança perante prestadores de serviços, parceiros e terceiros;

III. Apoiar a elaboração e revisão das comunicações regulatórias e institucionais aplicáveis;

IV. Orientar quanto à adoção de medidas judiciais, extrajudiciais ou administrativas, quando necessário; e

V. Acompanhar, quando aplicável, questões relacionadas à preservação da cadeia de custódia e validade jurídica das evidências coletadas.

5.9 Ponto Focal Responsável pela Proteção de Dados

Compete ao Encarregado:

I. Atuar como ponto de apoio junto ao DPO da Central,

II. Apoiar a avaliação do risco relevante aos titulares de dados pessoais ocasionado pelo incidente;

III. Apoiar as áreas responsáveis na análise das obrigações relacionadas à LGPD;

IV. Orientar as áreas internas acerca das medidas necessárias para mitigação dos impactos relacionados a dados pessoais; e

V. Acompanhar e apoiar o adequado registro do incidente para fins regulatórios e de governança.

5.10 Singulares

I. Reportar qualquer suspeita, indício ou identificação de incidente de segurança em seu ambiente tecnológico e infraestrutura local

II. Apoiar na contenção do incidente, quando este for tratado em conjunto com a Central;

III. Cumprir todas as diretrizes deste Plano com o intuito de tratar os incidentes visando o menor impacto possível;

IV. Designar responsável técnico para realizar tratativas referentes a este Plano (Marco Aurélio Martins – e-mail: greencred@greencred.com.br);

V. Designar responsável pela proteção de dados para realizar tratativas referentes a este Plano e apoiar o DPO quando os incidentes envolverem dados pessoais (Marcelo Kioshi Yamashita – e-mail: Marcelo.1074@greencred.com.br).

6 CICLO DE RESPOSTA A INCIDENTES

Uma vez identificado evento suspeito ou potencial incidente de segurança cibernética, o Diretor Responsável pela Segurança Cibernética deverá avaliar a necessidade de acionamento deste Plano e mobilização do Grupo de Trabalho para adoção das

medidas de análise, contenção, tratamento e recuperação aplicáveis (“Ciclo de Resposta a Incidentes”).

Em caso de suspeita, indício ou confirmação de incidente de segurança envolvendo o ambiente tecnológico ou a infraestrutura sob responsabilidade da cooperativa singular, esta deverá comunicar imediatamente a Central, por meio do canal oficial de e-mail: infosec@uniprimecentral.com.br.

A comunicação deverá conter informações suficientes e detalhadas sobre a ocorrência, de modo a subsidiar a análise do evento e, quando necessário, a constituição de grupo de trabalho conjunto para tratamento do incidente.

Após a análise e avaliação conjunta da ocorrência, a Central fornecerá as diretrizes e orientações para a condução da tratativa, podendo o tratamento ser realizado de forma centralizada, pela Central, ou pela própria cooperativa singular, conforme a natureza, criticidade e impacto do incidente identificado.

6.1 Detecção e Identificação

A detecção de incidentes poderá ocorrer por meio de mecanismos de monitoramento contínuo de eventos de segurança, análise de logs e trilhas de auditoria, geração de alertas automatizados por ferramentas especializadas, bem como por comunicações realizadas por colaboradores, prestadores de serviços, parceiros, cooperados ou autoridades competentes.

Todo evento suspeito, seja ele detectado de forma reativa ou proativa, deverá ser imediatamente registrado e tratado como potencial Incidente de Segurança até sua análise, validação e classificação pelo Grupo de Trabalho.

6.1.1 Análise e Classificação

Na etapa de análise, o Grupo de Trabalho deverá avaliar as evidências disponíveis, identificar a origem, extensão e natureza do Incidente de Segurança, bem como os

sistemas, serviços e dados potencialmente afetados. Deverão ser avaliados, no mínimo:

I. os impactos operacionais, financeiros, reputacionais e regulatórios decorrentes do Incidente de Segurança;
II. os efeitos sobre a confidencialidade, integridade, disponibilidade e autenticidade das informações;
III. a criticidade dos serviços, sistemas e processos impactados;
IV. o potencial impacto aos cooperados, parceiros e cooperativas filiadas e não filiadas;
V. a natureza dos dados potencialmente afetados, incluindo eventual envolvimento de dados sensíveis, financeiros, de autenticação ou demais hipóteses de risco ou dano relevante previstas na regulamentação da ANPD e BACEN.
VI. necessidade de contratação de equipe forense externa, se aplicável.

Na hipótese de um mesmo Incidente de Segurança apresentar características enquadráveis em mais de um nível de classificação, deverá prevalecer o nível de maior criticidade identificado pelo Grupo de Trabalho, inclusive nos casos em que o incidente envolva simultaneamente impactos operacionais e hipóteses de risco ou dano relevante aos titulares de dados pessoais previstas na regulamentação da ANPD.

Caso seja identificada, pelo Diretor Responsável pela Segurança Cibernética ou pelo Grupo de Trabalho, a necessidade de aprofundamento técnico para identificar a origem do Incidente, deverá ser prevista a contratação de serviço especializado para a realização desses estudos.

6.1.2 Classificação Sob A Perspectiva Do Banco Central Do Brasil (Bacen)

Com base nessa análise, o Incidente de Segurança deverá ser classificado de acordo com os níveis definidos na tabela abaixo, considerando o impacto na continuidade de

negócios da cooperativa:

Nível	Critérios
Baixo	Incidente restrito a ambientes internos ou sistemas de apoio, sem indícios de comprometimento de dados pessoais, credenciais privilegiadas, interrupção de serviços financeiros ou de pagamentos, necessidade de acionamento de contingência operacional ou impacto identificado a cooperados ou terceiros.
Médio	Incidente com indisponibilidade parcial de sistemas ou com comprometimento de dados pessoais que não envolva dados sensíveis, dados financeiros, dados de crianças, de adolescentes ou de idosos, dados de autenticação, dados protegidos por sigilo legal, judicial ou profissional, dados em larga escala; e sem indícios de interrupção de serviços financeiros ou de pagamentos.
Alto	Incidente com interrupção parcial de serviços financeiros ou de pagamentos; comprometimento de credenciais privilegiadas; necessidade de acionamento de contingência operacional; ou comprometimento de dados pessoais sensíveis, dados financeiros, dados de crianças, de adolescentes ou de idosos, dados de autenticação, dados protegidos por sigilo legal, judicial ou profissional, dados em larga escala, desde que não haja interrupção total ou severa da continuidade operacional da cooperativa.
Crítico	Incidente com interrupção total dos serviços financeiros ou de pagamentos; comprometimento da disponibilidade, integridade ou segurança dos serviços prestados por fornecedores relevantes; ou qualquer incidente com potencial de comprometer significativamente a continuidade, integridade, estabilidade ou segurança dos processos críticos da cooperativa.

Os incidentes classificados como **Críticos** configuram situação de crise e serão considerados **Incidentes Relevantes** para fins de reporte ao Banco Central do Brasil, na figura do Departamento de Supervisão de Cooperativas e Instituições não Bancárias (DESUC).

6.1.3 Classificação sob a Perspectiva da Agência Nacional de Proteção de Dados (ANPD)

Com base nessa análise, o Incidente de Segurança com dados pessoais deverá ser classificado de acordo com os critérios definidos em documento próprio que trata sobre dados pessoais.

6.2 Pré-Contenção

Para assegurar a validade jurídica, regulatória e a integridade das evidências coletadas durante o ciclo de resposta a um Incidente de Segurança, o Grupo de Trabalho e as demais áreas envolvidas deverão observar as seguintes diretrizes relativas ao tratamento forense e à manutenção da cadeia de custódia.

6.2.1 Preservação do Estado Original

Adoção de procedimentos técnicos formais para o isolamento lógico ou físico de ativos comprometidos, priorizando a coleta e preservação de evidências voláteis (como memória RAM e conexões ativas) e não voláteis (imagens de disco e *logs* de auditoria) antes de qualquer intervenção de recuperação ou restabelecimento do ambiente afetado.

6.2.2 Registro de Custódia

Documentação rigorosa, contínua e rastreável de todo o ciclo de vida da evidência, registrando formalmente a identificação dos Colaboradores que realizaram a coleta,

as transferências de posse, as datas e horários dos acessos, os métodos de extração utilizados e os locais de armazenamento.

6.2.3 Inalterabilidade das Evidências

Armazenamento seguro das provas digitais isoladas em repositórios segregados e protegidos, utilizando mecanismos de verificação de integridade (como a geração de algoritmos de *hash* criptográfico no momento da coleta) para garantir a inalterabilidade dos dados.

6.2.4 Restrição de Manuseio

Proibição expressa de manipulação, reinicialização ou exploração de equipamentos ou sistemas afetados por Colaboradores sem autorização prévia e competência técnica adequada, visando mitigar o risco de contaminação ou invalidação das evidências para fins de comprovação e responsabilização.

6.2.5 Apoio Especializado Externo

Nas hipóteses em que a investigação exigir alta complexidade técnica, ou quando a análise de dados tiver finalidade probatória para uso em eventuais processos legais ou judiciais de responsabilização, o Diretor Responsável pela Segurança Cibernética avaliará a contratação e o acionamento de investigadores forenses terceirizados e devidamente licenciados para conduzir as apurações.

6.3 Contenção

Finalizada a preservação das provas, o Grupo de Trabalho será responsável pela definição e execução das medidas de contenção necessárias à mitigação dos impactos decorrentes do Incidente de Segurança. A execução da contenção só poderá ser iniciada após avaliação e orientação da Uniprime Central Nacional para definição da ação a ser executada considerando o Risco Sistêmico.

Uma vez identificados indícios da origem, causa ou vetor de comprometimento do Incidente de Segurança, deverão ser adotadas, com maior brevidade possível, as medidas destinadas à contenção da ameaça, limitação dos impactos e preservação da continuidade operacional da Uniprime Greencred, sempre observada a necessidade de preservação das evidências para fins de investigações técnicas, análises forenses e regulatórias.

As medidas de contenção poderão incluir, dentre outras:

a) correção de vulnerabilidades identificadas;
b) bloqueio de funcionalidades, acessos ou credenciais;
c) desligamento controlado de sistemas ou serviços;
d) isolamento de ambientes, ativos, dispositivos ou usuários potencialmente comprometidos, inclusive mediante segmentação de rede;
e) proteção e segregação de ambientes de *backup* e recuperação;
f) alterações ou revogação de credenciais de acesso; e
g) adoção de quaisquer outras medidas técnicas ou operacionais necessárias à contenção, erradicação e posterior recuperação do Incidente de Segurança.

Quando o Incidente de Segurança envolver ou puder impactar o arranjo Pix ou outros arranjos de pagamentos, deverão ser observados, adicionalmente, os mecanismos, procedimentos e medidas específicas de contenção previstos na regulamentação aplicável.

6.4 Erradicação

Na sequência, será realizada a etapa de erradicação, que consiste na eliminação da causa raiz do incidente e na neutralização da ameaça no ambiente. Essa fase poderá envolver a remoção de códigos maliciosos, a correção de vulnerabilidades exploradas, a aplicação de atualizações e patches de segurança, a revisão de configurações inadequadas e o reforço de controles de acesso.

Visando a celeridade e a limitação de danos, a cooperativa deverá, sempre que possível, utilizar plataformas de Orquestração, Automação e Resposta de Segurança ou mecanismos automatizados para aplicar a reconfiguração dinâmica do ambiente (ex: isolamento de *endpoints*, bloqueios automáticos em *firewalls* ou revogação de privilégios de contas comprometidas). Adicionalmente, todo processo de erradicação deve ser validado para assegurar que nenhuma persistência do atacante ou artefato residual permaneça latente no sistema afetado.

A execução destas medidas poderá contar, quando necessário, com o apoio de serviços especializados, cuja contratação estará sujeita à prévia avaliação e aprovação da Central. Adicionalmente, conforme a gravidade, complexidade ou potencial risco sistêmico associado ao incidente, a Central poderá determinar a contratação de suporte técnico especializado específico, visando assegurar a adequada resposta, mitigação e continuidade operacional dos ambientes e sistemas envolvidos.

6.5 Recuperação

Após a erradicação, será iniciada a fase de recuperação, na qual os sistemas, serviços e dados afetados deverão ser restaurados de forma controlada e segura para um estado operacional.

Essa etapa inclui a recuperação de dados a partir de cópias de backup íntegras. É estritamente obrigatório que a integridade e a segurança dos ativos de restauração e dos backups sejam criptograficamente validadas e verificadas antes de sua utilização no ambiente de produção, visando impedir a reinfecção dos sistemas por malwares ou ataques de ransomware.

.

A reativação gradual dos serviços deverá respeitar os Tempos de Recuperação (RTO - Recovery Time Objective) e os Pontos de Recuperação (RPO - Recovery Point Objective) previamente estabelecidos para os Processos Críticos da cooperativa. Após a validação da consistência e integridade das informações, será realizado o

monitoramento reforçado dos ambientes, com o objetivo de identificar eventuais sinais de recorrência do incidente

Nos casos em que houver impacto relevante na disponibilidade dos serviços, deverão ser acionados os procedimentos previstos no Plano de Continuidade de Negócios (PCN) próprio ou Plano de Contingência de fornecedores.

6.6 Comunicação

Paralelamente às atividades técnicas de contenção e recuperação, deverá ser conduzido o fluxo de comunicação do Incidente de Segurança, observados os critérios de tempestividade, enquadramento e regras regulatórias aplicáveis ao caso concreto.

I. Comunicação interna e à alta administração

As comunicações relacionadas ao Incidente de Segurança deverão observar sua natureza, extensão, criticidade e potencial impacto operacional, regulatório ou reputacional, sendo direcionadas, conforme necessário, aos colaboradores, áreas responsáveis e alta administração.

As comunicações deverão conter nível de detalhamento compatível com as características do incidente e com o perfil dos destinatários, observadas a natureza das informações compartilhadas, as atribuições exercidas e a necessidade de conhecimento para o desempenho das respectivas funções.

As comunicações internas e à alta administração deverão ser alinhadas no âmbito do Grupo de Trabalho, com participação das áreas de Comunicação, Compliance e Jurídico.

II.Comunicação à Uniprime Central Nacional

Considerando a estrutura de governança e as diretrizes estabelecidas pela Política de Segurança Cibernética do Sistema Uniprime, as comunicações relacionadas ao Incidente de Segurança deverão observar sua natureza, extensão, criticidade e potencial impacto operacional, regulatório ou reputacional, sendo direcionadas à Uniprime Central Nacional com a máxima urgência e com nível de detalhamento em que seja possível o imediato entendimento do incidente.

III.Comunicação ao Banco Central do Brasil – DESUC

Os Incidentes de Segurança classificados como Críticos e afetem ou possam afetar o arranjo Pix, nos termos deste Plano, configuram incidentes relevantes para fins regulatórios e deverão ser comunicados tempestivamente ao Banco Central do Brasil.

A comunicação deverá ser realizada tão logo existam elementos mínimos que permitam o enquadramento dos Incidentes, ainda que a extensão dos impactos, a origem, a causa raiz ou demais informações não estejam integralmente confirmadas no momento do reporte inicial.

O reporte deverá ser conduzido pelo Diretor Responsável pelas áreas formalmente designados e cadastrados perante o Banco Central do Brasil para fins regulatórios, com apoio das áreas de Compliance e Jurídico, e deverá contemplar, sempre que possível, a descrição da natureza do incidente, os sistemas e serviços afetados, a estimativa de impactos e as medidas de contenção adotadas, podendo ser complementado por atualizações periódicas até a resolução do respectivo Incidente de Segurança.

IV.Comunicação aos usuários Pix potencialmente afetados

Nos casos de Incidentes de Segurança envolvendo componentes ou infraestrutura relacionados ao arranjo Pix, a cooperativa deverá observar os procedimentos

operacionais aplicáveis à comunicação de usuários pessoas físicas potencialmente afetados, nos termos da regulamentação do Banco Central do Brasil aplicável ao Pix.

V.Comunicação à Agência Nacional de Proteção de Dados - ANPD

A comunicação à Agência Nacional de Proteção de Dados (ANPD) é obrigatória em caso de incidentes que acarretam risco ou dano relevante para titulares de dados. O processo de comunicação à ANPD deverá seguir as regras descritas em documento próprio e em conjunto com o DPO.

VI.Comunicação aos Instituidores de Arranjos de Pagamentos

As áreas de Jurídico e Compliance deverão avaliar as obrigações de comunicação decorrentes dos Incidentes de Segurança perante os instituidores dos arranjos de pagamento dos quais a cooperativa seja participante, observados os critérios, prazos, procedimentos e requisitos previstos nos contratos, regulamentos e manuais operacionais aplicáveis.

VII.Comunicação à imprensa e comunicações públicas

Na hipótese de incidente de segurança com repercussão pública ou necessidade de comunicação externa, as manifestações institucionais deverão ser coordenadas pelo Grupo de Trabalho, com apoio das áreas de Comunicação, Compliance e Jurídico, observando os fluxos internos de aprovação e os impactos técnicos, regulatórios, operacionais e reputacionais envolvidos.

Todas as comunicações públicas e aos órgãos reguladores, devem ser poiadas e avaliadas em conjunto com a Uniprime Central Nacional considerando o Risco Sistêmico.

6.7 Registros e Relatórios

Todos os Incidentes de Segurança, independentemente de sua classificação ou enquadramento como incidente relevante, deverão ser formalmente registrados em sistema, ferramenta ou repositório próprio destinado ao controle e rastreabilidade dos Incidentes de Segurança.

As cooperativas singulares serão responsáveis por realizar e manter os registos de incidentes identificados em sua infraestrutura e manter a documentação à disposição da Uniprime Central Nacional.

O registro deverá conter, no mínimo, as seguintes informações, quando disponíveis:

a) Introdução, Metodologia e Objetivos
b) Data e hora da detecção do Incidente de Segurança;
c) Cronologia do incidente
d) Forma de identificação do Incidente de Segurança;
e) Descrição do Incidente de Segurança e dos eventos associados;
f) Sistemas, serviços, ambientes, operações e dados potencialmente afetados;
g) Identificação das evidências digitais coletadas, com a documentação de quem as coletou, métodos de extração utilizados e local de armazenamento seguro, atestando a inalterabilidade para fins de processos legais ou regulatórios
h) Extratos específicos dos registros de eventos (*logs*) que detectaram e/ou corroboraram o incidente, contendo, no mínimo, a identificação do usuário/sistema, a data e hora exatas, o endereço de origem e o tipo de evento ocorrido.
i) Detalhamento técnico dos artefatos utilizados pelo atacante, visando retroalimentar e fortalecer os sistemas de "Caça" a Ameaças da Cooperativa.
j) Classificação atribuída ao Incidente de Segurança e respectivos critérios considerados para seu enquadramento;
k) Avaliação preliminar e atualização dos impactos operacionais, financeiros, reputacionais e regulatórios identificados;

l) Indicação de eventual impacto a cooperados, terceiros, cooperativas filiadas e não filiadas ou usuários de serviços financeiros e de pagamento;
m) Medidas de contenção, erradicação, recuperação e mitigação adotadas;
n) Registros das comunicações internas e externas realizadas, incluindo comunicações regulatórias, quando aplicável;
o) Indicação das áreas envolvidas no tratamento do Incidente de Segurança;
p) Identificação da causa raiz, quando possível;
q) Data de resolução; e
r) Lições aprendidas e eventuais medidas de aprimoramento identificadas e/ou implementadas.

Os registros deverão ser mantidos de forma íntegra, rastreável e acessível pelo prazo mínimo previsto na regulamentação aplicável, inclusive para fins de atendimento a solicitações das autoridades competentes, auditorias internas e externas e demais procedimentos de supervisão e controle.

6.7.1 Registro do Incidente sob a perspectiva do Banco Central do Brasil

Além dos registros internos, os Incidentes de Segurança classificados como “Críticos”, nos termos deste Plano, ocorridos até a data-base de 31 de dezembro deverão compor o relatório anual sobre a implementação do Plano de Ação e de Resposta a Incidentes, o qual deverá ser submetido à aprovação do Conselho de Administração, e na sua ausência da Diretoria Executiva, até 31 de março do exercício subsequente e mantido à disposição do Banco Central do Brasil. O referido relatório deverá contemplar, no mínimo:

a) a efetividade da implementação do presente Plano;
b) o resumo das ações, procedimentos, controles e tecnologias utilizados na prevenção e resposta a incidentes;
c) os resultados dos testes de intrusão e dos testes, varreduras e análises periódicas para detecção de vulnerabilidades realizados no período, acompanhados dos respectivos planos de ação estabelecidos para a correção das vulnerabilidades identificadas;

d) os Incidentes de Segurança classificados como “Críticos” ocorridos no período;
e) os principais impactos identificados e medidas adotadas;
f) os resultados dos testes de continuidade de negócios relacionados a Incidentes de Segurança; e
g) os planos de ação e medidas de aprimoramento implementados ou previstos.

7 TRATAMENTO DE CENÁRIOS ESPECÍFICOS

O Ciclo de Resposta a Incidentes previsto neste Plano aplica-se a todos os Incidentes de Segurança, independentemente de sua natureza, origem ou classificação.

Os cenários descritos neste tópico estabelecem procedimentos, controles e medidas complementares aplicáveis conforme o tipo de Incidente de Segurança identificado na etapa de Análise e Classificação, os quais deverão ser observados em conjunto com as etapas gerais do Ciclo de Resposta a Incidentes.

Os Incidentes de Segurança que não se enquadrem especificamente nos cenários abaixo permanecerão integralmente sujeitos às diretrizes e procedimentos gerais previstos neste Plano.

7.1 Vulnerabilidades

Nos Incidentes de Segurança originados ou agravados por vulnerabilidades, deverão ser observados adicionalmente:

I. A classificação da vulnerabilidade conforme seu nível de criticidade considerando os impacto e riscos associados;
II. A definição de plano de ação para correção ou mitigação, com estabelecimento de SLA compatível com a criticidade identificada;
III. O registro, rastreabilidade e acompanhamento da vulnerabilidade até sua efetiva resolução, incluindo eventual monitoramento de efeitos residuais após

a contenção inicial.

7.2 Indisponibilidade de Serviços de TI

Nos Incidentes de Segurança enquadrados como nível “Crítico” em razão de impactos na continuidade das operações da cooperativa, deverão ser observados adicionalmente:

I. A avaliação da indisponibilidade dos serviços afetados, especialmente nos casos de:
   a) interrupção total de Processos Críticos ou de serviços prestados por Fornecedores Relevantes ou; ou
   b) interrupção parcial de Processos Críticos ou de serviços prestados por Fornecedores Relevantes.
II. A integração com o PCN, assegurando alinhamento entre a recuperação de serviços e a continuidade das operações; e
III. A adoção de medidas de correção e recuperação compatíveis com os níveis de serviço aplicáveis, incluindo monitoramento até a plena restauração da capacidade operacional.

7.3 Vazamento de Dados e Informações

Em casos de incidentes que envolvam o vazamento de dados e informações, o tratamento deve considerar:

I. Aplicação de mecanismos de detecção de incidentes;
II. Contenção imediata do vazamento conforme SLA definido;
III. Acionamento do Ciclo de Resposta a Incidentes;
IV. Identificação da origem e extensão do incidente;
V. Realização da análise do incidente para determinar a natureza, a categoria e a quantidade de titulares de dados afetados;
VI. Avaliação do impacto, dos riscos e os danos potenciais aos titulares dos dados;

VII. Comunicação do incidente seguindo os níveis de severidade e critérios de relevância, garantindo reporte tempestivo às partes internas e externas aplicáveis, quando necessário, incluindo a elaboração de plano de comunicação para as autoridades competentes.

7.4 Corrupção de Dados

Nos Incidentes de Segurança que envolvam a corrupção de dados ou comprometimento de integridade das informações, deverão ser observados adicionalmente:

I. O isolamento dos sistemas e ambientes afetados, de forma a prevenir a propagação da corrupção e preservar as evidências para análise da causa raiz;
II. A identificação da origem do problema, realizando um diagnóstico para determinar a extensão da corrupção, os dados impactados e a causa do Incidente de Segurança, utilizando os registros de acesso, se necessário;
III. A adoção de procedimentos de restauração segura dos dados a partir de cópias de backup íntegras e confiáveis, incluindo, quando aplicável, integração com o Plano de Continuidade de Negócios;
IV. Após a restauração, a realização de testes de validação para assegurar a integridade e a consistência dos dados recuperados antes do restabelecimento integral das operações e sistemas;
V. A revisão de processos e controles e mecanismos de proteção relacionados ao Incidente de Segurança, com definição de medidas preventivas e de aprimoramento.

7.5 Incidentes com *Ransomware*

Em casos de Incidentes de Segurança ocasionados por *ransomware*, deverão ser observados adicionalmente:

I. O isolamento imediato de todos os sistemas e segmentos de rede afetados para conter a propagação da ameaça e proteger os backups;
II. A identificação da variante do ransomware e a extensão do impacto, determinando quais dados foram criptografados e se há evidências de exfiltração, destruição ou comprometimento de dados, sistemas e serviços;
III. A não realização de pagamento de resgate como postura padrão da ***, salvo decisão formal, excepcional e fundamentada da alta administração;
IV. A ativação, quando aplicável, do PCN, incluindo procedimentos de erradicação do malware e restauração dos sistemas e dados a partir de backups íntegros e seguros, conforme avaliação da estratégia de não pagamento de resgate;
V. A observância dos fluxos de comunicação e reporte previstos neste Plano, inclusive quando houver impactos relacionados à continuidade operacional, dados pessoais, serviços financeiros ou obrigações regulatórias aplicáveis.

7.6 Incidentes envolvendo fornecedores e prestadores de serviços

Nos casos de Incidentes de Segurança que envolvam fornecedores ou prestadores de serviços, deverão ser observados os procedimentos escalonamento, comunicação, contenção e gestão contratual aplicáveis, incluindo eventual acionamento do fornecedor/prestador responsável, avaliação de impactos às integrações e adoção de medidas necessárias à mitigação dos riscos operacionais e regulatórios decorrentes do referido incidente.

Após o tratamento do Incidente de Segurança, deverá ser realizada avaliação do desempenho do fornecedor ou prestador de serviços envolvido, podendo resultar na aplicação de medidas contratuais, revisão de controles, reavaliação do enquadramento como Fornecedor Relevante, quando aplicável, ou revisão da continuidade do relacionamento.

8 CONTINUIDADE DE NEGÓCIOS

O presente Plano integra a estrutura de continuidade de negócios da Cooperativa *** e deverá ser aplicado de forma coordenada com o Plano de Continuidade de Negócios e os demais normativos internos relacionados à segurança cibernética, continuidade operacional e recuperação de ambientes tecnológicos.

Na hipótese de o Incidente de Segurança ocasionar impactos que se enquadrem nos critérios de acionamento do PCN, o referido normativo deverá ser ativado de forma concomitante ao presente Plano, observados os respectivos fluxos de escalonamento, contingência, recuperação e continuidade operacional aplicáveis ao caso concreto.

A atuação coordenada entre este Plano, o PCN deverá buscar assegurar a mitigação dos impactos operacionais, a preservação das atividades críticas e a retomada segura dos serviços e operações.

9 TREINAMENTO E CONSCIENTIZAÇÃO

A cooperativa deverá promover ações contínuas de treinamento, capacitação e conscientização relacionadas à segurança cibernética, conforme disposto na Política de Segurança Cibernética.

Adicionalmente, deverão ser realizados testes periódicos de efetividade deste Plano, incluindo simulações, exercícios práticos e cenários de crise e demais eventos relevantes à continuidade operacional.

Os resultados dos treinamentos, testes e simulações deverão ser formalmente registrados e utilizados para revisão, aprimoramento contínuo dos controles internos, atualização dos procedimentos de resposta e fortalecimento da cultura de segurança cibernética.

10 ATIVIDADES PÓS-INCIDENTE DE SEGURANÇA E MELHORIA CONTÍNUA

Após o encerramento do Incidente de Segurança, o Grupo de Trabalho deverá avaliar a efetividade das medidas de resposta adotadas, os impactos observados, os controles utilizados e as oportunidades de aprimoramento identificadas durante o tratamento do Incidente de Segurança.

Deverão ser registradas, sempre que aplicável:

a) Os pontos de melhoria identificados nos processos, controles e mecanismos de prevenção e resposta;
b) As recomendações para mitigação de riscos e prevenção de recorrência de Incidentes de Segurança similares; e
c) A cronologia dos principais eventos, ações e decisões relacionadas ao Incidente de Segurança.

As lições aprendidas decorrentes dos Incidentes de Segurança deverão ser utilizadas para revisão e aprimoramento contínuo deste Plano, dos controles internos, dos procedimentos operacionais, dos mecanismos de prevenção e das ações de conscientização e treinamento relacionadas à segurança cibernética.

11 GUARDA E ARMAZENAMENTO DE DOCUMENTOS

Os documentos relacionados a este Plano, incluindo o próprio Plano e suas versões anteriores, os registros de Incidentes de Segurança, os relatórios anuais e a documentação relativa aos critérios que configurem situação de crise, deverão ser mantidos à disposição do Banco Central do Brasil pelo prazo mínimo de 5 (cinco) anos.

12 ATUALIZAÇÃO E DIVULGAÇÃO

Esta Plano deverá ser revisada em conjunto com a Política de Segurança Cibernética no mínimo anualmente, ou sempre que houver alterações na legislação aplicável ou mudanças nas práticas de negócios, e aprovado pelo Conselho de Administração ou, na sua ausência, pela Diretoria Executiva.

Quadro de Atualizações

Criação do Plano
Estruturação completa.
Aprovada em 17/08/2026