POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão: 1.0

Data de Aprovação: 10/10/2025

Data da Última Revisão: 10/10/2025

SUMÁRIO

RESUMO

Este resumo apresenta os princípios e compromissos fundamentais da Política de Segurança e Resiliência Cibernética da Cooperativa de Crédito Rural Seara - Crediseara. Em um cenário de crescentes ameaças cibernéticas, a proteção dos ativos de informação e a continuidade das operações são prioridades estratégicas e inegociáveis para a cooperativa.

A Política de Segurança e Resiliência Cibernética da Crediseara estabelece as diretrizes para garantir a confidencialidade, integridade e disponibilidade das informações de nossos associados e da própria instituição. Ela atende integralmente aos requisitos da legislação e regulamentação vigentes, especialmente a Resolução CMN nº 4.893/2021 e a Lei Geral de Proteção de Dados (LGPD).

Nossa abordagem é proativa e baseada em riscos, focando na prevenção de incidentes e fraudes, no monitoramento contínuo e na capacidade de resposta eficaz. A política define uma estrutura de governança clara, com papéis e responsabilidades bem estabelecidos para o Conselho de Administração, Diretoria Executiva, comitês e todas as áreas da cooperativa.

A Crediseara implementa controles de segurança robustos, incluindo gestão de acesso com autenticação multifator, criptografia de dados em trânsito e em repouso, proteção contra softwares maliciosos e gerenciamento rigoroso de cópias de segurança (backups). Um Plano de Resposta a Incidentes Cibernéticos (PRI) formal e abrangente, juntamente com Planos de Continuidade de Negócios (PCN) testados e integrados a serviços de terceiros, assegura a nossa capacidade de recuperação e resiliência operacional frente a eventos adversos.

Reconhecemos a importância do relacionamento seguro com terceiros, garantindo que nossos requisitos de segurança se estendem a fornecedores e prestadores de serviços por meio de avaliações de risco e cláusulas contratuais claras. A conscientização e o treinamento contínuo de todos os colaboradores são pilares para a construção de uma cultura de segurança forte, complementada por canais de comunicação claros para o reporte de incidentes.

Este documento representa o compromisso da Crediseara com a excelência em segurança e resiliência cibernética, garantindo a proteção de nossos associados e a sustentabilidade de nossas operações no ambiente digital.

1. DISPOSIÇÕES GERAIS

Esta seção estabelece o propósito fundamental, a aplicabilidade, as responsabilidades de alto nível e os princípios orientadores da Política de Segurança e Resiliência Cibernética da Crediseara. Ela serve como a base conceitual que sustenta todas as diretrizes e ações subsequentes.

1.1. Área responsável

a) O conselho de administração é o responsável pela aprovação final de política.

b) A Diretoria Executiva é a área responsável pela criação, supervisão e garantia da manutenção contínua desta Política de Segurança e Resiliência Cibernética.

c) A Diretoria Administrativa é a responsável pela política.

d) A área de Tecnologia da Informação e Segurança Cibernética é responsável pela elaboração, implementação e gestão diária das diretrizes, procedimentos e controles decorrentes desta política.

1.2. Abrangência

a) Esta Política orienta o comportamento e as diretrizes de segurança cibernética em todos os níveis da Cooperativa de Crédito Rural Seara - Crediseara.

b) Aplica-se a todos os colaboradores da Crediseara bem como a associados, prestadores de serviços, fornecedores e quaisquer terceiros que, direta ou indiretamente, interajam com os ativos de informação da cooperativa ou que executem atividades em seu nome.

c) O escopo desta política engloba todos os ativos de informação da Crediseara, incluindo, mas não se limitando a: dados, sistemas, aplicações, infraestrutura de tecnologia da informação, dispositivos e informações armazenadas em qualquer formato ou meio.

1.3. Regulamentação

1.3.1. Conformidade com as leis, normas e regulamentos

Esta Política de Segurança e Resiliência Cibernética está em conformidade com as seguintes leis, normas e regulamentos, sendo o mínimo a ser observado pela Cooperativa:

a) Resolução CMN nº 4.893, de 26 de fevereiro de 2021: Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

b) Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD): Que dispõe sobre o tratamento de dados pessoais.

c) Resolução CMN nº 4.606, de 25 de setembro de 2017: Que dispõe sobre a política de segurança cibernética e a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras.

d) Resolução CMN nº 5.051/2022: Que dispõe sobre a organização e o funcionamento de cooperativas de crédito.

1.4. Periodicidade de revisão

Esta Política, bem como seu Manual de Segurança Cibernética complementar, será revisada, no mínimo, anualmente ou extraordinariamente, a qualquer tempo, conforme estabelecido no Art. 10 da Resolução CMN nº 4.893/2021.

1.5. Efetividade da revisão

A efetividade da revisão será comprovada através de registros formais da diretoria executiva e de aprovação pelo Conselho de Administração quando necessário.

1.6. Classificação da informação

Todos os dados e informações da Crediseara são considerados ativos valiosos e serão classificados de acordo com sua sensibilidade, criticidade e impacto potencial em caso de acesso indevido, alteração ou indisponibilidade.

A classificação das informações será definida nas seguintes categorias, que serão detalhadas em procedimento específico (Manual de Classificação da Informação), incluindo diretrizes para seu manuseio, armazenamento, acesso, compartilhamento e descarte:

a) Pública: Informações de livre divulgação que não causariam dano à cooperativa caso se tornassem públicas. São dados destinados ao conhecimento geral.

b) Interna: Informações destinadas ao consumo exclusivo e uso interno da Crediseara. Embora não sejam confidenciais, sua divulgação externa não autorizada pode causar desconforto ou pequena desvantagem operacional.

c) Confidencial: Informações sensíveis da cooperativa ou de seus associados, cujo acesso não autorizado, modificação ou divulgação pode causar dano moderado, financeiro, reputacional ou legal. Exige controle de acesso rigoroso.

d) Restrita/Secreta: Informações de altíssima criticidade, cujo acesso não autorizado, modificação ou divulgação causaria danos severos ou catastróficos à Crediseara, incluindo perda financeira substancial, graves impactos reputacionais, sanções regulatórias pesadas ou comprometimento da continuidade do negócio.

1.7. Princípios da segurança cibernética

As ações de segurança e resiliência cibernética na Crediseara serão norteados pelos seguintes princípios fundamentais:

a) Gestão de Riscos: A segurança cibernética é gerenciada com base na identificação, avaliação e tratamento contínuo dos riscos aos ativos de informação da cooperativa.

b) Prevenção: Adotar e manter mecanismos de prevenção a incidentes, fraudes, danos, perdas, erros e ataques cibernéticos.

c) Monitoramento Contínuo: Implementar e utilizar processos, controles e tecnologias para monitorar de forma contínua o ambiente e responder a ataques cibernéticos.

d) Resposta Eficaz: Estabelecer rotinas e procedimentos para cenários de incidentes relevantes, garantindo a capacidade de detectar, conter, erradicar e se recuperar rapidamente.

e) Disseminação da Cultura: Disseminar a cultura de segurança cibernética por meio de sensibilização, conscientização e capacitação contínua de todos os envolvidos.

f) Relacionamento Seguro: Preservar os requisitos de segurança cibernética na contratação de serviços ou pessoas e no relacionamento com funcionários, fornecedores, terceiros, parceiros, contratados e estagiários.

g) Controle de Acesso Individualizado: Disponibilizar, controlar e rastrear os acessos individuais para cada usuário, de acordo com as suas responsabilidades.

h) Continuidade de Negócios: A segurança cibernética é parte integrante da gestão da continuidade de negócios, assegurando a resiliência operacional.

i) Comprometimento da Alta Administração: A alta gestão demonstra e fomenta ativamente o compromisso com a segurança cibernética em toda a organização.

j) Melhoria Contínua: Promover a evolução constante das práticas de segurança, incorporando lições aprendidas e adaptando-se às novas ameaças e tecnologias.

2. GOVERNANÇA DA SEGURANÇA CIBERNÉTICA

Este capítulo define a estrutura organizacional, os processos e as responsabilidades para a gestão, supervisão e avaliação da segurança e resiliência cibernética na Crediseara. Ele assegura que a segurança cibernética esteja alinhada aos objetivos estratégicos da cooperativa e em conformidade com as regulamentações vigentes.

2.1. Estratégia de Segurança Cibernética

A estratégia de segurança cibernética da Crediseara é um componente essencial da estratégia geral de negócios, garantindo que a proteção dos ativos de informação e a resiliência operacional sejam prioridades contínuas.

2.1.1. Alinhamento com os objetivos da cooperativa

A segurança e resiliência cibernética são fundamentais para o atingimento dos objetivos estratégicos da Crediseara, protegendo a reputação, a continuidade dos serviços, a confiança dos associados e o valor da cooperativa. A estratégia de segurança cibernética apoia diretamente a missão de garantir um ambiente seguro para as operações financeiras e a proteção dos dados pessoais e financeiros dos associados.

2.1.2. Definição de papéis e responsabilidades

A responsabilidade pela segurança e resiliência cibernética é compartilhada em toda a cooperativa. As atribuições são definidas da seguinte forma:

a) Conselho de Administração: Responsável pela aprovação da Política de Segurança e Resiliência Cibernética, do Plano de Resposta a Incidentes Cibernéticos e do Plano de Continuidade de Negócios. Supervisiona a gestão dos riscos cibernéticos e aloca os recursos necessários.

b) Diretoria Executiva: Garante a implementação e o cumprimento desta Política. Aprova planos de ação, aloca recursos operacionais e promove a cultura de segurança.

c) Comitê de Segurança Cibernética: Órgão colegiado multidisciplinar responsável por analisar, discutir e recomendar diretrizes e planos de ação específicos em segurança cibernética, reportando-se à Diretoria Executiva.

d) Gestor de Segurança Cibernética (ou profissional/equipe designada): Responsável pela elaboração, implementação e manutenção atualizada da Política, manuais e procedimentos, gestão de riscos cibernéticos, coordenação da resposta a incidentes e dos programas de conscientização e treinamento. Também monitora o cumprimento da política e garante a conformidade regulatória.

e) Líderes e Gestores de Área: Asseguram a aplicação das diretrizes em suas áreas, promovem a conscientização, e garantem o reporte e tratamento de vulnerabilidades e incidentes em suas respectivas competências.

f) Colaboradores (em todos os níveis): São responsáveis por compreender e aderir às diretrizes da Política, proteger os ativos de informação sob sua custódia e reportar imediatamente incidentes ou atividades suspeitas.

2.1.3. Processo de gestão de riscos cibernéticos

A Crediseara desenvolve um processo contínuo de gestão de riscos cibernéticos, que envolve a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos associados aos ativos de informação da cooperativa. Este processo está detalhado no Manual de Segurança Cibernética e observa as seguintes etapas:

a) Identificação: Mapeamento de ameaças e vulnerabilidades que podem afetar a confidencialidade, integridade e disponibilidade dos ativos.

b) Avaliação: Análise da probabilidade de ocorrência dos riscos e do impacto potencial em caso de concretização, utilizando métodos qualitativos e quantitativos.

c) Tratamento: Definição e implementação de controles e medidas para mitigar, transferir, aceitar ou evitar os riscos identificados.

d) Monitoramento: Acompanhamento contínuo da eficácia dos controles, do cenário de riscos e das novas ameaças.

e) Comunicação: Reporte regular sobre a postura de risco cibernético à Diretoria Executiva e ao Conselho de Administração.

2.2. Supervisão da Segurança Cibernética

A supervisão da segurança cibernética garante que as diretrizes estabelecidas sejam efetivamente implementadas e que a postura de segurança da cooperativa seja continuamente aprimorada.

2.2.1. Responsabilidades da Diretoria Executiva e do Conselho de Administração

A Diretoria Executiva e o Conselho de Administração são as instâncias máximas de governança pela segurança cibernética.

a) Conselho de Administração: Aprova esta Política e os planos estratégicos de segurança cibernética, incluindo o Plano de Resposta a Incidentes e o Plano de Continuidade de Negócios. Garante que a cooperativa possua recursos adequados para a gestão da segurança cibernética e monitora os relatórios de risco e incidentes.

b) Diretoria Executiva: Assegura a execução das políticas e planos aprovados, e supervisiona a gestão de riscos de TI e os controles de segurança da informação.

2.2.2. Mecanismos de acompanhamento e avaliação da eficácia da política

A Crediseara conta com mecanismos formais para acompanhar e avaliar a eficácia desta Política e dos controles de segurança cibernética, incluindo:

a) Relatórios Periódicos: Elaboração de relatórios internos de desempenho de segurança cibernética para a Diretoria Executiva e o Conselho de Administração.
b) Auditorias Internas e Externas: Realização de auditorias periódicas para verificar a conformidade e a eficácia dos controles.
c) Análise de Incidentes: Utilização das lições aprendidas com incidentes de segurança para identificar falhas e aprimorar a política e os procedimentos.
d) Avaliações de Risco: Revisão regular do cenário de riscos cibernéticos para ajustar as estratégias e controles.

2.3. Plano de Ação e Resposta a Incidentes

A Crediseara mantém um Plano de Resposta a Incidentes Cibernéticos (PRI) formal e abrangente, que detalha os procedimentos para se preparar, detectar, analisar, conter, erradicar, recuperar e comunicar incidentes de segurança cibernética, em conformidade com o Art. 6º da Resolução CMN nº 4.893/2021. Este plano é aprovado pelo Conselho de Administração.

2.3.1. Preparação para Incidentes

A Crediseara tem uma postura proativa para a gestão de incidentes cibernéticos.

2.3.1.1. Definição de critérios para classificação de incidentes

Serão estabelecidos critérios claros e padronizados para a classificação de incidentes de segurança cibernética com base em sua criticidade, impacto potencial (financeiro, reputacional, operacional, legal) e sensibilidade dos dados envolvidos. A classificação orientará a priorização das ações de resposta.

2.3.1.2. Estabelecimento de equipes de resposta a incidentes

Estão designadas formalmente equipes de resposta a incidentes relevantes (internas ou com o apoio de terceiros especializados), com responsabilidades, funções e treinamentos específicos para agir em diferentes cenários deste nível de incidentes cibernéticos.

2.3.1.3. Desenvolvimento de planos de comunicação

A cooperativa conta com planos e modelos de comunicação específicos para diferentes tipos de incidentes, definindo:

a) Públicos-alvo

b) Canais de comunicação

c) Mensagens-chave e porta-vozes autorizados

2.3.2. Detecção e Análise

A Crediseara mantém mecanismos para a detecção tempestiva de incidentes cibernéticos e a análise de eventos de segurança.

2.3.2.1. Implementação de ferramentas de monitoramento de segurança

São utilizadas ferramentas de monitoramento de segurança para coletar, analisar e correlacionar eventos de segurança em tempo real, permitindo a detecção de anomalias e atividades suspeitas em sistemas, redes e aplicações.

2.3.2.2. Procedimentos para análise de logs e eventos de segurança

A Crediseara conta com procedimentos formais para a análise de logs de sistemas, rede e aplicações, bem como de outros eventos de segurança, visando identificar potenciais incidentes, determinar sua natureza e extensão.

2.3.2.3. Mecanismos para identificação de incidentes em tempo real

A cooperativa contém mecanismos para identificação de incidentes em tempo real, incluindo alertas automatizados baseados em padrões de ameaças, inteligência de ameaças e monitoramento contínuo do ambiente.

2.3.3. Resposta e Recuperação

A Crediseara mantém uma postura de melhoria contínua de aumento da capacidade de responder rapidamente incidentes cibernéticos, minimizando os impactos.

2.3.3.1. Procedimentos para contenção, erradicação e recuperação de incidentes

A Crediseara mantém procedimentos detalhados para cada fase da resposta a incidentes, incluindo:

a) Contenção: Isolamento de sistemas, redes ou contas comprometidas para impedir a propagação do incidente.

b) Erradicação: Remoção da causa raiz do incidente e de elementos maliciosos do ambiente.

c) Recuperação: Restauração de sistemas e serviços afetados para o seu estado operacional normal.

2.3.3.2. Restauração de sistemas e serviços afetados

A Crediseara implementa planos de restauração para sistemas e serviços críticos, garantindo a recuperação tempestiva e a validação da integridade dos dados e da funcionalidade após um incidente cibernético, com base em objetivos de tempo de recuperação (RTO) e ponto de recuperação (RPO).

2.3.4. Comunicação de incidentes às partes interessadas

A Crediseara estabelece procedimentos formais e ágeis para a comunicação de incidentes relevantes às partes interessadas, em conformidade com as regulamentações vigentes:

a) Banco Central do Brasil (BCB): Comunicação tempestiva de incidentes relevantes, conforme Art. 20, inciso III, da Resolução CMN nº 4.893/2021.

b) Autoridade Nacional de Proteção de Dados (ANPD): Notificação de incidentes que possam acarretar risco ou dano relevante aos titulares de dados pessoais, conforme a LGPD (Art. 48).

c) Associados: Comunicação clara e transparente sobre incidentes que os afetem, com orientações sobre medidas de proteção, quando aplicável.

d) Imprensa e Público Geral: Gerenciamento da comunicação para preservar a reputação da cooperativa.

e) Colaboradores e Liderança Interna: Manter informadas as equipes e a alta gestão sobre o status do incidente.

2.3.5. Testes periódicos dos planos de resposta

Os Planos de Resposta a Incidentes Cibernéticos são testados e simulados periodicamente, incluindo testes de mesa e simulações mais complexas com as equipes envolvidas, para validar sua efetividade e identificar pontos de melhoria. Os resultados desses testes serão documentados e utilizados para aprimorar o plano.

2.4. Auditoria da Segurança Cibernética

A Crediseara assegura a avaliação independente da efetividade de sua política e controles de segurança cibernética.

2.4.1. Realização de auditorias internas e externas

Serão realizadas auditorias internas e, quando cabível, externas (Auditoria Cooperativa), para avaliar a aderência da cooperativa a esta Política, aos procedimentos internos e às regulamentações do Banco Central do Brasil. O escopo e a periodicidade das auditorias serão definidos com base na relevância e no risco.

2.4.2. Acompanhamento e correção das não conformidades identificadas

A Crediseara estabelece um processo formal para o registro, acompanhamento e correção das não conformidades, deficiências e achados de auditoria relacionados à segurança cibernética. As ações corretivas terão responsáveis e prazos definidos, e sua efetividade será monitorada.

3. GESTÃO DE RISCOS CIBERNÉTICOS

Este capítulo estabelece a metodologia e os processos para a gestão de riscos cibernéticos na Crediseara. A cooperativa adota uma abordagem baseada em riscos para a segurança cibernética, garantindo que os esforços e investimentos em segurança sejam direcionados às ameaças e vulnerabilidades mais relevantes, alinhando-se aos objetivos de negócio e às exigências regulatórias.

3.1. Processo de Identificação de Riscos

A Crediseara mantém um processo formal e contínuo para a identificação de riscos cibernéticos, abrangendo todos os ativos de informação e suas interações no ambiente da cooperativa.

3.1.1. Identificação de ativos de informação, ameaças e vulnerabilidades

A cooperativa identifica e documenta todos os ativos de informação relevantes, incluindo sistemas, aplicações, infraestrutura, dados em repouso e em trânsito e dispositivos. Para cada ativo, são identificadas as ameaças potenciais e as vulnerabilidades existentes que podem comprometer a confidencialidade, integridade e disponibilidade das informações.

3.1.2. Avaliação do impacto nos negócios e na reputação da cooperativa

A Crediseara avalia o impacto potencial que a materialização de cada risco cibernético pode causar aos negócios da cooperativa, incluindo perdas financeiras, interrupção de serviços, danos à reputação, prejuízos à imagem institucional e violações legais ou regulatórias (como sanções do Banco Central ou multas da LGPD).

3.2. Avaliação e Priorização de Riscos

A Crediseara avalia e prioriza os riscos cibernéticos identificados para direcionar os recursos de forma eficaz e garantir que os riscos mais críticos sejam tratados primeiramente.

3.2.1. Metodologia para avaliar a probabilidade e o impacto dos riscos

A cooperativa utiliza uma metodologia padronizada para avaliar a probabilidade de ocorrência de cada risco cibernético e o seu impacto potencial, conforme identificado no item 3.1.2. Esta metodologia emprega critérios qualitativos e/ou quantitativos que permitem uma análise consistente dos riscos.

3.2.2. Definição de critérios para priorizar os riscos a serem tratados

Com base na avaliação de probabilidade e impacto, a Crediseara define critérios claros para a priorização dos riscos cibernéticos. Os riscos são classificados em níveis de criticidade para determinar a urgência e a alocação de recursos necessários para o seu tratamento, garantindo que os riscos com maior potencial de dano sejam mitigados prioritariamente.

3.3. Tratamento de Riscos

A Crediseara implementa estratégias para tratar os riscos cibernéticos identificados, buscando reduzir sua exposição a níveis aceitáveis.

3.3.1. Definição de controles e medidas de segurança

Para cada risco cibernético identificado e priorizado, a cooperativa define e documenta as estratégias de tratamento, que podem incluir:

a) Mitigação: Implementação de controles e medidas de segurança (técnicas, físicas ou processuais) para reduzir a probabilidade de ocorrência ou o impacto do risco.

b) Transferência: Contratação de seguros ou terceirização de serviços com cláusulas de responsabilidade para transferir parte do risco.

c) Aceitação: Decisão formal de aceitar um risco que se encontra dentro dos limites de apetite a risco da cooperativa, após análise custo-benefício.

d) Evitar: Alteração de processos ou tecnologias para eliminar completamente o risco.

3.3.2. Implementação de planos de ação para tratar os riscos prioritários

A Crediseara elabora e executa planos de ação específicos para implementar os controles e medidas de tratamento dos riscos cibernéticos prioritários. Esses planos definem responsáveis, prazos, recursos necessários e indicadores de progresso, garantindo que as ações sejam realizadas de forma efetiva e monitorada.

3.4. Monitoramento e Revisão de Riscos

A Crediseara mantém um processo contínuo de monitoramento e revisão da gestão de riscos cibernéticos para adaptar-se a um ambiente de ameaças em constante evolução e garantir a eficácia dos controles.

3.4.1. Monitoramento contínuo dos riscos e da eficácia dos controles

A cooperativa realiza o monitoramento contínuo dos riscos cibernéticos e da efetividade dos controles de segurança implementados. Isso inclui a análise de indicadores de segurança, relatórios de incidentes, resultados de varreduras de vulnerabilidade e o acompanhamento de novas ameaças cibernéticas.

4. CONTROLES DE SEGURANÇA CIBERNÉTICA

Este capítulo define os controles e as medidas técnicas, operacionais e administrativas que a Crediseara implementa para proteger seus ativos de informação contra ameaças cibernéticas. Estes controles são essenciais para garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas da cooperativa.

4.1. Controle de Acesso

A Crediseara implementa controles rigorosos para gerenciar e monitorar o acesso a seus ativos de informação, assegurando que apenas usuários autorizados acessem os recursos necessários para suas funções.

4.1.1. Identificação e Autenticação

A cooperativa adota procedimentos formais para a identificação e autenticação de usuários em todos os sistemas e redes.

4.1.1.1. Procedimentos para cadastro e descadastramento de usuários

A Crediseara mantém procedimentos documentados para o cadastro, alteração e descadastramento de usuários em todos os sistemas, plataformas e redes, garantindo que os acessos são concedidos e revogados de forma tempestiva e controlada, conforme as necessidades de negócio.

4.1.1.2. Políticas de senhas fortes e gestão de senhas

A cooperativa estabelece e aplica políticas de senhas que exigem complexidade mínima, rotação periódica e proíbem o reuso de senhas anteriores. Incentiva e orienta os colaboradores sobre as melhores práticas de gestão e proteção de senhas.

4.1.1.3. Implementação de autenticação multifator

A Crediseara implementa e mantém mecanismos de autenticação multifator (MFA) para todos os acessos relevantes a sistemas e aplicações visando fortalecer a verificação da identidade dos usuários, quando esta tecnologia de autenticação está disponível.

4.1.2. Gerenciamento de privilégios de acesso

A Crediseara adota o princípio do menor privilégio, concedendo aos usuários apenas os acessos estritamente necessários para o desempenho de suas funções. Implementa o controle de autorização baseado em perfis de acesso (RBAC) e mecanismos formais de segregação de funções, a fim de mitigar o risco de acessos indevidos ou incompatíveis com as atribuições dos usuários.

4.1.3. Revisão periódica dos acessos

A cooperativa realiza revisões periódicas das permissões de acesso em sistemas e bases de dados críticos, a fim de garantir que os acessos concedidos continuam alinhados às responsabilidades dos usuários e que credenciais inativas ou desnecessárias são revogadas, conforme o Art. 3º, § 2º da Resolução CMN nº 4.893/2021.

4.2. Proteção contra Malware

A Crediseara implementa múltiplas camadas de proteção para mitigar os riscos associados a softwares maliciosos e outras ameaças cibernéticas.

4.2.1. Implementação de software antivírus e antimalware

A cooperativa utiliza e mantém software antivírus e antimalware atualizado em todos os endpoints (servidores, estações de trabalho e notebooks) e sistemas aplicáveis da sua infraestrutura tecnológica.

4.2.2. Atualização regular das assinaturas de malware

A Crediseara assegura a atualização regular das assinaturas e bases de dados dos softwares antivírus e antimalware, bem como a aplicação de pacotes e correções de segurança nos sistemas operacionais e aplicações, para garantir a proteção contra as ameaças mais recentes.

4.2.3. Prevenção de execução de códigos maliciosos

A cooperativa implementa medidas técnicas e processuais para prevenir a execução não autorizada de códigos maliciosos, incluindo filtros de e-mail, controle de navegação web, e mecanismos de detecção e prevenção de intrusões (IDS/IPS) na rede.

4.3. Segurança da Rede

A Crediseara adota controles de segurança robustos para proteger sua infraestrutura de rede, controlando o fluxo de informações e prevenindo acessos não autorizados.

4.3.1. Segmentação da rede

A cooperativa segmenta sua rede em zonas de segurança distintas para isolar sistemas críticos e dados sensíveis. Esta segmentação limita o impacto de potenciais ataques e restringe o movimento lateral de atacantes em caso de comprometimento.

4.3.2. Firewalls e sistemas de detecção de intrusão

A Crediseara utiliza firewalls de rede e sistemas de detecção e prevenção de intrusões (IDS/IPS) para monitorar e controlar o tráfego de rede, bloqueando acessos não autorizados e detectando atividades suspeitas ou maliciosas.

4.3.3. Proteção de redes sem fio

A cooperativa implementa controles de segurança para suas redes sem fio (Wi-Fi), incluindo autenticação robusta, criptografia do tráfego e segmentação da rede sem fio da rede corporativa principal, para prevenir acessos não autorizados.

4.4. Criptografia

A Crediseara emprega mecanismos de criptografia para proteger a confidencialidade e a integridade de seus dados mais sensíveis, tanto em trânsito quanto em repouso.

4.4.1. Criptografia de dados em trânsito e em repouso

A cooperativa implementa e mantém mecanismos de criptografia para proteger dados em trânsito (durante a transmissão por redes) e dados em repouso (armazenados em servidores, bancos de dados, dispositivos e serviços em nuvem), conforme exigido pelo Art. 3º, § 2º da Resolução CMN nº 4.893/2021 e Art. 46, § 1º da Lei nº 13.709/2018 (LGPD).

4.5. Segurança em Nuvem (Quando Aplicável)

Ao utilizar serviços de computação em nuvem, a Crediseara adota medidas específicas para garantir a segurança dos dados e serviços hospedados.

4.5.1. Responsabilidades compartilhadas de segurança

A Crediseara compreende e documenta as responsabilidades compartilhadas de segurança entre a cooperativa e o provedor de serviços em nuvem, definindo claramente quais aspectos da segurança são de sua responsabilidade e quais são do provedor, conforme Art. 12 da Resolução CMN nº 4.893/2021.

4.5.2. Configuração segura de serviços em nuvem

A cooperativa implementa e monitora a configuração segura de todos os serviços em nuvem utilizados, aplicando as melhores práticas e diretrizes de segurança do provedor, a fim de minimizar vulnerabilidades e exposições.

4.5.3. Proteção de dados na nuvem

A Crediseara garante que os dados armazenados e processados em ambientes de nuvem são protegidos com controles adequados, incluindo criptografia, controle de acesso e monitoramento, em conformidade com as exigências regulatórias e as políticas internas de classificação da informação.

4.6. Segurança de Dispositivos Móveis

A Crediseara estabelece diretrizes para o uso seguro de dispositivos móveis, sejam eles corporativos ou pessoais, que acessam os ativos de informação da cooperativa.

4.6.1. Políticas para uso de dispositivos móveis corporativos e pessoais

A cooperativa mantém políticas claras que regem o uso de dispositivos móveis (smartphones, tablets, notebooks) corporativos e pessoais (BYOD - Bring Your Own Device) para acesso a informações da Crediseara, definindo regras para segurança de senhas, instalação de aplicativos, acesso a redes Wi-Fi e manuseio de dados sensíveis.

Inclui-se nestas políticas a restrição ou proibição do uso de dispositivos de armazenamento portáteis não autorizados em equipamentos e redes corporativas.

4.6.2. Gerenciamento de dispositivos móveis (MDM)

A Crediseara utiliza soluções de gerenciamento de dispositivos móveis (MDM) para aplicar políticas de segurança, configurar dispositivos, monitorar a conformidade, e, quando necessário, realizar o apagamento remoto de dados corporativos em caso de perda ou roubo.

4.7. Cópias de Segurança (Backup)

A Crediseara mantém um programa de cópias de segurança para garantir a disponibilidade e a integridade dos dados e a recuperação de sistemas em caso de incidentes.

4.7.1. Políticas e procedimentos para geração de cópias de segurança

A cooperativa estabelece e segue políticas e procedimentos detalhados para a realização de cópias de segurança (backups) de todos os dados e sistemas críticos do ambiente de rede e sistemas corporativos. Esses procedimentos definem a frequência, o método, o local de armazenamento e o período de retenção dos backups.

4.7.2. Testes periódicos de restauração do ambiente

A Crediseara realiza testes periódicos e documentados de restauração a partir das cópias de segurança, abrangendo o ambiente de rede e sistemas corporativos. Esses testes visam validar a integridade dos backups e a capacidade da cooperativa de restaurar dados e sistemas de forma eficaz e tempestiva em cenários de perda de dados ou indisponibilidade, conforme Art. 3º, § 2º da Resolução CMN nº 4.893/2021. Os resultados desses testes são registrados e utilizados para aprimoramento contínuo dos processos de backup e restauração.

5. RESILIÊNCIA CIBERNÉTICA E CONTINUIDADE DE NEGÓCIOS

Este capítulo define as diretrizes para a Crediseara assegurar a resiliência de suas operações e a continuidade dos negócios frente a incidentes cibernéticos ou outras interrupções. A cooperativa mantém uma estrutura para se preparar, detectar, resistir, responder e se recuperar de eventos adversos, minimizando seus impactos e protegendo a integridade e a disponibilidade de seus serviços.

5.1. Planos de Continuidade de Negócios (PCN)

A Crediseara estabelece e mantém um Plano de Continuidade de Negócios (PCN) formal e atualizado, que é parte integrante de sua estratégia de resiliência cibernética. Este plano visa garantir o reinício ou a normalização tempestiva dos serviços relevantes em caso de interrupção ou desastre.

5.1.1. Procedimentos para assegurar a continuidade dos serviços relevantes em caso de incidentes

A cooperativa desenvolve procedimentos detalhados e específicos para assegurar a continuidade dos serviços considerados relevantes e críticos para suas operações, mesmo diante de incidentes cibernéticos ou outros eventos disruptivos. O PCN define os objetivos de tempo de recuperação (RTO - Recovery Time Objective) e os objetivos de ponto de recuperação (RPO - Recovery Point Objective) para esses serviços, orientando as ações de recuperação para minimizar o tempo de inatividade e a perda de dados.

5.1.2. Testes periódicos dos PCN

A Crediseara executa testes periódicos e documentados dos Plano de Continuidade de Negócios (PCN). Esses testes validam a efetividade dos procedimentos de continuidade e recuperação e a resiliência da infraestrutura tecnológica frente a

cenários de interrupção, como ataques cibernéticos em massa. Os resultados dos testes são registrados e utilizados para aprimoramento contínuo dos planos.

5.1.3. Estratégias para garantir a resiliência dos serviços terceirizados

A cooperativa integra formalmente o plano de continuidade da Crediseara com os planos dos prestadores de serviços críticos, cuja interrupção pode impactar diretamente suas operações. Esta integração inclui:

a) Análise de riscos associada
b) Avaliação de impactos
c) Realização de testes conjuntos e validações práticas.

A Crediseara assegura que os contratos com terceiros relevantes contemplem cláusulas de resiliência e continuidade de negócios.

5.2. Gerenciamento de Crises Cibernéticas

A Crediseara mantém um processo formal e uma estrutura definida para o gerenciamento de crises resultantes de incidentes cibernéticos, com o objetivo de minimizar os impactos negativos e restaurar a normalidade operacional e a confiança.

5.2.1. Procedimentos para gerenciar eventos que possam causar impactos significativos na cooperativa

A cooperativa estabelece procedimentos claros para o gerenciamento de crises cibernéticas que podem acarretar impactos significativos, como:

a) Perdas financeiras substanciais
b) Danos reputacionais severos
c) Interrupção prolongada de serviços essenciais
d) Violações legais

Estes procedimentos definem a composição da equipe de gestão de crise, a cadeia de comando, as rotinas de decisão, a alocação de recursos emergenciais e as etapas para escalonamento e resolução da crise.

O Plano de Resposta a Incidentes Cibernéticos (PRI) é parte fundamental deste gerenciamento.

5.2.2. Comunicação com as partes interessadas durante crises cibernéticas

A Crediseara estabelece e formaliza planos de comunicação para gerenciar a informação durante crises cibernéticas, em conformidade com as exigências regulatórias e de boas práticas. A comunicação ocorre de forma tempestiva, transparente e direcionada às seguintes partes interessadas:

a) Banco Central do Brasil (BCB): Notificação obrigatória de incidentes relevantes, conforme Art. 20, inciso III, da Resolução CMN nº 4.893/2021.

b) Autoridade Nacional de Proteção de Dados (ANPD): Notificação de incidentes que possam acarretar risco ou dano relevante aos titulares de dados pessoais, conforme a LGPD (Art. 48).

c) Associados: Fornecimento de informações claras, concisas e orientações sobre medidas de proteção, quando aplicável e relevante.

d) Imprensa e Público Geral: Gerenciamento proativo da imagem institucional, com porta-vozes definidos e mensagens alinhadas.

e) Colaboradores e Liderança Interna: Manutenção de comunicação interna eficaz para garantir a coordenação e o alinhamento de todos os envolvidos na resposta à crise.

6. CONSCIENTIZAÇÃO E TREINAMENTO

A Crediseara reconhece que a conscientização e a capacitação contínua de todos os colaboradores são essenciais para a construção de uma cultura de segurança cibernética robusta e para a efetividade de seus controles. Este capítulo estabelece as diretrizes para o programa de conscientização e treinamento da cooperativa.

6.1. Programa de Conscientização em Segurança Cibernética

A cooperativa mantém um programa abrangente de conscientização em segurança cibernética, que visa educar e capacitar todos os colaboradores sobre as melhores práticas de segurança e os riscos cibernéticos.

6.1.1. Treinamentos periódicos para os colaboradores sobre temas relevantes de segurança

A Crediseara oferece treinamentos periódicos e obrigatórios para todos os colaboradores, abordando temas relevantes de segurança cibernética.

Esses treinamentos incluem, mas não se limitam a:

a) Identificação de ataques de phishing e engenharia social
b) Uso seguro de senhas, proteção de dados pessoais e informações sensíveis
c) Uso seguro de dispositivos e sistemas
d) Processo de reporte de incidentes.

A cooperativa utiliza plataformas de capacitação e métodos variados.

6.1.2. Simulações de phishing e outros ataques para testar a conscientização dos colaboradores

A cooperativa realiza simulações controladas de ataques cibernéticos, como campanhas de phishing e engenharia social, para testar a conscientização e a capacidade dos colaboradores em identificar e reagir a tentativas maliciosas. Os

resultados dessas simulações são analisados para identificar pontos de melhoria no programa de conscientização e para reforçar o aprendizado.

6.1.3. Comunicação regular de informações sobre segurança cibernética

A Crediseara mantém canais de comunicação regulares para disseminar informações importantes sobre segurança cibernética. Isso inclui o envio de alertas sobre novas ameaças, dicas de segurança, e a disponibilização de materiais educativos que reforçam as diretrizes da Política de Segurança e Resiliência Cibernética.

6.2. Capacitação Técnica e Profissionalização

A Crediseara assegura a capacitação técnica contínua dos profissionais diretamente responsáveis pela segurança cibernética e pela gestão de tecnologia da informação.

- Identificação Formal dos Responsáveis: A cooperativa identifica formalmente os profissionais internos responsáveis pela segurança cibernética e suas atribuições, garantindo a rastreabilidade das ações de qualificação e a governança sobre o tema.
- Desenvolvimento de Competências: A cooperativa promove o desenvolvimento de competências técnicas específicas em segurança cibernética para sua equipe, com registro das ações realizadas e alinhamento ao plano de ação e à política de segurança da cooperativa.

7. RELACIONAMENTO COM TERCEIROS

A Crediseara reconhece que a segurança da cadeia de suprimentos e o relacionamento com terceiros relevantes são componentes críticos de sua postura de segurança cibernética.

A cooperativa estabelece diretrizes para garantir que os requisitos de segurança e resiliência cibernética sejam preservados e cumpridos na contratação e gestão de fornecedores, prestadores de serviços, parceiros relevantes que direta ou indiretamente interajam com seus ativos de informação.

7.1. Requisitos de Segurança na Contratação de Serviços Relevantes

A cooperativa adota um processo formal para a contratação de serviços relevante, especialmente aqueles que envolvem processamento, armazenamento de dados e computação em nuvem, garantindo que os riscos de segurança cibernética sejam devidamente avaliados e mitigados.

7.1.1. Avaliação dos riscos de segurança cibernética na contratação de fornecedores e prestadores de serviços relevantes

A Crediseara formaliza, com base em critérios objetivos e riscos identificados, a avaliação de relevância de todas as contratações de serviços que envolvam processamento e/ou armazenamento de dados e computação em nuvem.

Esta avaliação é fundamental para:

a) Subsidiar as decisões de contratação
b) Garantir que os riscos associados sejam adequadamente gerenciados, conforme exigido pelos Arts. 11 e 12 da Resolução CMN nº 4.893/2021.

A cooperativa elabora e implementa uma política formal que estabelece critérios e procedimentos para:

a) Avaliação da capacidade de prestadores relevantes de serviços de tecnologia

b) Assegurar a confidencialidade, integridade, disponibilidade e recuperação de dados e informações processados ou armazenados.

As avaliações dos contratos em vigor com prestadores relevantes são formalizadas retroativamente.

7.1.2. Definição de cláusulas de segurança nos contratos com terceiros relevantes

A cooperativa assegura que os contratos com fornecedores e prestadores de serviços relevantes que interagem com seus ativos de informação contêm cláusulas de segurança cibernética explícitas.

Estas cláusulas definem:

a) As responsabilidades de ambas as partes em relação à segurança da informação
b) Requisitos de conformidade
c) Notificação de incidentes
d) Direitos de auditoria
e) Garantias sobre a proteção de dados pessoais e operacionais.

7.1.3. Monitoramento do cumprimento dos requisitos de segurança por parte dos terceiros relevantes

A Crediseara implementa mecanismos para o monitoramento contínuo do cumprimento dos requisitos de segurança cibernética por parte de seus fornecedores e prestadores de serviços.

Este monitoramento inclui a verificação da aderência às políticas e procedimentos de segurança estabelecidos.

A cooperativa estabelece procedimentos formais para o aceite documental da Política de Segurança Cibernética por parte das empresas terceirizadas que desempenham funções críticas ou que tratam de dados sensíveis.

8. CANAL DE COMUNICAÇÃO

A Crediseara estabelece canais de comunicação claros e acessíveis para que colaboradores, associados e terceiros possam reportar alertas e incidentes de segurança cibernética, garantindo uma resposta rápida e eficaz a potenciais ameaças.

8.1. Canal para Alerta de Segurança e Incidentes

A cooperativa disponibiliza canais de comunicação dedicados para o reporte de alertas de segurança e/ou incidentes cibernéticos. A Crediseara divulga amplamente os seguintes canais entre todos os seus colaboradores, associados e parceiros, assegurando que o processo de reporte é claro e encorajado, sem receios de retaliação.

9. RESPONSABILIDADES

Este capítulo detalha as responsabilidades específicas de cada nível e área da Crediseara em relação à segurança e resiliência cibernética, reforçando que a proteção dos ativos de informação é um compromisso coletivo da cooperativa.

9.1. Diretor Responsável pela Política

O Diretor Administrativo é o responsável pela supervisão e garantia do cumprimento desta Política de Segurança e Resiliência Cibernética, atuando como o ponto focal da alta gestão para o tema.

9.2. Responsabilidades das Áreas de Negócio

Cada área de negócio da Crediseara é responsável por:

a) Compreender e aplicar as diretrizes desta Política e dos procedimentos de segurança cibernética relacionados às suas operações.

b) Garantir que as informações sob sua custódia são classificadas e manuseadas de acordo com as diretrizes estabelecidas.

c) Promover a conscientização sobre segurança cibernética junto às suas equipes.

d) Assegurar que vulnerabilidades e incidentes de segurança cibernética identificados em suas áreas são reportados tempestivamente à área de Tecnologia da Informação e Segurança Cibernética.

e) Participar ativamente na gestão de riscos operacionais relacionados à TI em suas respectivas áreas.

9.3. Responsabilidades da Área de Tecnologia e Segurança Cibernética

A área de Tecnologia da Informação e Segurança Cibernética é responsável por:

a) Elaborar, implementar e manter atualizada esta Política, o Manual de Segurança Cibernética e todos os procedimentos e planos operacionais relacionados.

b) Implementar e manter os controles técnicos e operacionais de segurança cibernética.

c) Realizar o monitoramento contínuo do ambiente de TI para detecção de ameaças e incidentes.

d) Promover e coordenar os programas de conscientização e treinamento em segurança cibernética para toda a cooperativa.

e) Gerenciar o relacionamento com fornecedores de tecnologia, assegurando a conformidade com os requisitos de segurança.

9.4. Responsabilidades dos Colaboradores

Todos os colaboradores da Crediseara, independentemente de sua função ou nível hierárquico, são responsáveis por:

a) Compreender e aderir rigorosamente às diretrizes estabelecidas nesta Política e nos demais procedimentos de segurança cibernética.

b) Proteger os ativos de informação da cooperativa sob sua responsabilidade e custódia.

c) Reportar imediatamente quaisquer incidentes de segurança, vulnerabilidades ou atividades suspeitas por meio do canal de comunicação apropriado.

d) Participar ativamente dos treinamentos e programas de conscientização em segurança cibernética.

e) Utilizar os recursos de tecnologia da informação da cooperativa de forma ética e segura, em conformidade com as políticas de uso.

10. HISTÓRICO DE REVISÕES

Este capítulo registra o histórico de elaboração, revisão e atualização da Política de Segurança e Resiliência Cibernética da Crediseara, garantindo a rastreabilidade das alterações e a transparência do processo de gestão do documento.

10.1. Registro de Elaboração, Revisão e Atualização

A cooperativa mantém um registro formal de todas as versões desta política, incluindo:

a) Data: Data da alteração ou revisão.

b) Descrição: Detalhamento das modificações realizadas, incluindo a justificativa para as alterações.

c) Aprovação: Referência ao órgão de governança (ex: Conselho de Administração) e número da ata de aprovação (se aplicável).

VERSÃO	DATA	DESCRIÇÃO	APROVAÇÃO
1.0	10/2025	Reestruturação da política.	Ata 485

11. GLOSSÁRIO E ACRÔNIMOS

A.

Ameaça: Potencial causa de um incidente indesejado que pode resultar em dano para um sistema ou organização.

ANPD (Autoridade Nacional de Proteção de Dados): Órgão da administração pública federal responsável por fiscalizar e regular a Lei Geral de Proteção de Dados (LFPD).

Antimalware: Software projetado para detectar, prevenir e remover softwares maliciosos (malware), incluindo vírus, worms, trojans, spyware e ransomware.

Ativo de Informação: Qualquer informação ou sistema de informação que tenha valor para a cooperativa e, portanto, necessita de proteção. Isso inclui dados, sistemas de hardware e software, serviços e pessoas.

Auditoria Interna: Atividade de avaliação independente e objetiva, concebida para agregar valor e melhorar as operações de uma organização. No contexto de segurança, verifica a conformidade e a eficácia dos controles.

Autenticação Multifator (MFA): Método de segurança que exige que os usuários provem sua identidade por meio de duas ou mais credenciais de verificação diferentes, como senha e código enviado ao celular.

B.

Backup: Cópia de segurança de dados ou sistemas, realizada para que possam ser restaurados em caso de perda, corrupção ou indisponibilidade dos dados originais.

BCB (Banco Central do Brasil): Autarquia federal que atua como principal autoridade monetária do país e regulamenta e fiscaliza instituições financeiras e de pagamento.

BYOD (Bring Your Own Device): Política que permite que colaboradores utilizem seus dispositivos móveis pessoais (smartphones, tablets, notebooks) para fins relacionados ao trabalho.

C.

CMN (Conselho Monetário Nacional): Órgão máximo do Sistema Financeiro Nacional, responsável por formular a política da moeda e do crédito.

Confidencialidade: Propriedade que assegura que a informação não é disponibilizada ou revelada a indivíduos, entidades ou processos não autorizados.

Continuidade de Negócios: Capacidade de uma organização de continuar a entregar produtos ou serviços em níveis aceitáveis previamente definidos, após um incidente disruptivo.

Controle de Acesso: Mecanismo que restringe a entrada em um determinado local ou o uso de um recurso, sistema ou informação a usuários autorizados.

Corrupção de Dados: Erros nos dados ou na sua manipulação que causam modificações não autorizadas ou perda de integridade dos dados, tornando-os incorretos ou inutilizáveis.

Criptografia: Processo de codificação de informações de forma que apenas as partes autorizadas possam decifrá-las e compreendê-las, protegendo a confidencialidade e a integridade dos dados.

Crise Cibernética: Evento cibernético de grande magnitude que causa impacto significativo nas operações, reputação, finanças ou conformidade de uma organização.

D.

Disponibilidade: Propriedade que assegura que usuários autorizados tenham acesso à informação e aos ativos correspondentes quando necessário.

E.

Engenharia Social: Manipulação psicológica de pessoas para que elas realizem ações ou divulguem informações confidenciais, muitas vezes usadas em ataques cibernéticos.

Endpoint: Qualquer dispositivo final conectado a uma rede (computador, notebook, servidor, dispositivo móvel).

F.

Firewall: Dispositivo ou software que atua como barreira de segurança, controlando o tráfego de rede e impedindo acessos não autorizados entre redes ou sistemas.

Fraude em Massa: Esquemas fraudulentos que visam um grande número de vítimas, muitas vezes utilizando engenharia social e meios digitais.

G.

Gestão de Riscos Cibernéticos: Processo sistemático de identificação, avaliação, tratamento, monitoramento e comunicação de riscos associados a ameaças e vulnerabilidades cibernéticas.

I.

IDS/IPS (Intrusion Detection System / Intrusion Prevention System): Sistema de Detecção de Intrusões / Sistema de Prevenção de Intrusões. Ferramentas que monitoram o tráfego de rede em busca de atividades maliciosas ou violações de política, podendo alertar (IDS) ou bloquear (IPS) tais atividades.

Incidente Cibernético: Qualquer evento adverso relacionado à segurança de sistemas de informação que comprometa ou ameace comprometer a confidencialidade, integridade ou disponibilidade de ativos de informação.

Integridade: Propriedade que salvaguarda a exatidão e a completão da informação e dos ativos.

Inteligência de Ameaças (Threat Intelligence): Conhecimento baseado em evidências, incluindo contexto, mecanismos, indicadores, implicações e recomendações acionáveis sobre ameaças existentes ou emergentes.

L.

LGPD (Lei Geral de Proteção de Dados Pessoais): Lei brasileira (Lei nº 13.709/2018) que regulamenta o tratamento de dados pessoais por pessoas físicas ou jurídicas de direito público ou privado.

Log: Registro cronológico de eventos e atividades ocorridas em sistemas, redes ou aplicações, essencial para auditoria e investigação de incidentes.

M.

Malware: Termo genérico para software malicioso, incluindo vírus, worms, trojans, ransomware e spyware.

MDM (Mobile Device Management): Gerenciamento de Dispositivos Móveis. Soluções que permitem controlar, configurar e proteger smartphones, tablets e outros dispositivos móveis utilizados na organização.

P.

PCN (Plano de Continuidade de Negócios): Documento que detalha os procedimentos e estratégias para garantir a continuidade das operações essenciais de uma organização após um evento disruptivo.

Pentest (Teste de Penetração): Simulação de um ataque cibernético contra um sistema de computador, rede ou aplicativo web, para verificar vulnerabilidades que poderiam ser exploradas.

Phishing: Ataque de engenharia social que tenta enganar usuários para que revelem informações confidenciais (senhas, dados financeiros) ou instalem software malicioso, geralmente por meio de e-mails, mensagens ou sites falsos.

Privilégio Mínimo: Princípio de segurança que estabelece que um usuário, programa ou processo deve ter apenas os privilégios mínimos necessários para executar sua função.

PRI (Plano de Resposta a Incidentes Cibernéticos): Documento que estabelece os procedimentos e as diretrizes para a preparação, detecção, análise, contenção, erradicação, recuperação e comunicação de incidentes de segurança cibernética.

R.

Ransomware: Tipo de malware que criptografa os arquivos do usuário ou do sistema, bloqueando o acesso, e exige um resgate (geralmente em criptomoedas) para liberá-los.

RBAC (Role-Based Access Control): Controle de Acesso Baseado em Papéis. Modelo de controle de acesso onde as permissões são associadas a papéis (funções) dentro da organização, e os usuários recebem permissões através da atribuição a esses papéis.

Resiliência Cibernética: Capacidade de uma organização de se preparar, detectar, resistir, responder e se recuperar de incidentes cibernéticos, mantendo a entrega dos resultados desejados, mesmo sob estresse.

RPO (Recovery Point Objective): Objetivo de Ponto de Recuperação. A quantidade máxima de dados que uma organização está disposta a perder em caso de um desastre. Determina a frequência dos backups.

RTO (Recovery Time Objective): Objetivo de Tempo de Recuperação. O tempo máximo aceitável para restaurar um serviço ou sistema após uma interrupção.

S.

SDLC (Software Development Life Cycle): Ciclo de Vida de Desenvolvimento de Software. Processo que abrange todas as fases do desenvolvimento de software, desde a concepção até a manutenção.

Secure SDLC: Integração de práticas e requisitos de segurança em cada fase do Ciclo de Vida de Desenvolvimento de Software.

Segregação de Funções: Princípio de controle que visa reduzir o risco de fraude ou erro ao dividir as tarefas críticas entre diferentes indivíduos, impedindo que uma única pessoa controle um processo completo e sensível.

SIEM (Security Information and Event Management): Gerenciamento de Informações e Eventos de Segurança. Sistema que coleta e analisa dados de logs e eventos de segurança de diversas fontes para identificar atividades suspeitas e alertar sobre incidentes.

Simulação de Ataque: Exercício controlado que replica táticas, técnicas e procedimentos de ataque cibernético para testar as defesas e a capacidade de resposta da organização.

T.

Testes de Mesa (Tabletop Exercises): Exercícios de discussão sobre cenários de incidentes ou desastres, usados para validar planos e responsabilidades sem impactar as operações reais.

TLS/SSL (Transport Layer Security / Secure Sockets Layer): Protocolos criptográficos que fornecem segurança de comunicação pela internet para aplicações como e-mail, navegação web e mensagens instantâneas.

Trilha de Auditoria: Registro sequencial das atividades em um sistema ou rede, que permite rastrear eventos até sua origem, essencial para investigação e responsabilização.

V.

Vulnerabilidade: Fraqueza ou falha em um sistema, controle, processo ou projeto que pode ser explorada por uma ameaça para causar dano.