1. OBJETIVO

Estabelecer os princípios, diretrizes, responsabilidades e controles mínimos obrigatórios destinados à prevenção, detecção, resposta e mitigação de riscos cibernéticos, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações e dos sistemas da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A., em conformidade com a **Resolução CMN nº 4.893/2021, e sua complementar a Resolução CMN nº 5.274/2025**.

Diante do exposto, esta política tem por objetivo:

a) Estabelecer controles para segurança das informações corporativas através dos requisitos de Confidencialidade, Integridade e Disponibilidade, Autenticidade e Rastreabilidade;

b) Transformar as estratégias de gestão da segurança da informação em ações;

c) Demonstrar o comprometimento da instituição com as questões de proteção de informações.

2. ESCOPO

Aplica-se a:

- Todos os colaboradores (CLT, PJ, estagiários, temporários);
- Conselheiros e Diretores;
- Terceiros e prestadores de serviço;
- Sistemas internos e externos;
- Ambientes em nuvem;
- Infraestrutura crítica e sistemas de pagamento.

3. CONCEITO

3.1. Segurança da Informação

É a preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, como autenticidade, responsabilidade, não-repúdio e confiabilidade.

3.2. Ativos

São bens que tem valor para a organização e necessitam ser protegidos. A informação é um ativo, e assim como outros, essenciais para o negócio, motivo pelo qual precisa ser adequadamente protegida.

3.3. Propriedade

As informações e os ativos de informações processados, armazenados e/ou trafegados através de recursos tecnológicos ou meios físicos da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A. são de propriedade da Instituição. A utilização deles por qualquer usuário está sujeita ao cumprimento das disposições desta Política e de suas respectivas Normas e Procedimentos.

3.4. Gestor do Ativo de Informação

Colaborador ou área responsável por um ou mais ativos de informação ou processo na estrutura da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A. Normalmente, se caracterizam por gestores ou colaboradores que respondem por áreas funcionais e com responsabilidades de definição dos critérios de proteção alinhados com as diretivas de segurança da instituição.

3.5. Usuário

Para efeitos desta política, são aqueles que utilizam ativos de informação para o desempenho de suas funções na UY3 SOCIEDADE DE CRÉDITO DIRETO S.A.

4. Diretrizes

4.1. Acesso as Informações

O acesso à informação de propriedade da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A. deve ser permitido somente a usuários autorizados pelo proprietário da informação,

levando em consideração o princípio de menor privilégio, segregação de funções conflitantes e a classificação da informação.

Ao manipular informações ou sistemas de informações da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A, o usuário deve ter ciência desta Política de Segurança da Informação entendendo suas diretrizes e certificar-se de que toda atividade não claramente explicita é expressamente proibida.

4.2. Identificação de Usuário

A UY3 SOCIEDADE DE CRÉDITO DIRETO S.A. estabelece como regra o acesso a sistemas de processamento de informações com identificação pessoal, inequívoca e intransferível. O compartilhamento de credenciais de acesso a todo e qualquer sistema de informações ou ferramenta tecnológica é expressamente proibido.

4.3. Uso de Credenciais (Senhas)

Os usuários devem utilizar senhas seguras, com palavras não vinculadas a instituição ou vida pessoal (aniversários, nome de filhos, pets entre outros), que facilitem sua predição. As senhas utilizadas devem obrigatoriamente seguir os seguintes critérios: conter entre 8 e 16 caracteres, ter ao menos uma (01) letra maiúscula, uma (01) letra minúscula, um (01) caractere especial e um (01) numeral. As senhas devem ser alteradas a cada 90 dias, não sendo permitido a reutilização das últimas doze (12) senhas anteriores.

4.4. Uso de Softwares

É vedado o uso de softwares de terceiros não homologados pela TI e aprovados pela Segurança da Informação da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A.

4.5. Reporte de Incidentes

Os comportamentos de ataques são identificados pelos meios de detecção implementados no ambiente (antivírus, antispam, filtro de conteúdo, correlacionamento de logs, entre outros).

Outros eventos, atitudes suspeitas ou incidentes de segurança devem ser reportados ao time de Segurança da Informação **(seguranca@uy3.com.br)**.

4.6. Segurança Física e do Ambiente

O acesso físico a ambientes de armazenamento de informações sensíveis deve ser restrito.

Todos os usuários definidos no âmbito desta Política devem adotar a prática de manter seus ambientes de trabalho organizados, com as informações, independentemente de sua forma de representação, armazenadas em locais seguros. Os computadores devem ter as telas bloqueadas sempre que o usuário se ausentar de sua posição de trabalho.

4.7. Privacidade das Informações

Todos os colaboradores presentes no escopo desta política devem prezar pelo sigilo e privacidade das informações da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A., evitando o compartilhamento de informações confidenciais com usuários ou terceiros não autorizados.

4.8. Gestão de Fornecedores e Terceiros

Todo fornecedor e terceiro contratado pela UY3 SOCIEDADE DE CRÉDITO DIRETO S.A., devem zelar pela privacidade e segurança das informações as quais possui acesso durante a vigência de seu contrato com a Instituição.

Após o fim do vínculo, todos dados gerados e armazenados pelo fornecedor ou terceiro em seu equipamento devem ser excluídos e não devem ser utilizados pelo mesmo para qualquer fim, salvo se expressamente autorizado pela Diretoria da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A.

Os fornecedores e terceiros devem manter seu equipamento com seu sistema operacional atualizado, software contra vírus e malwares instalado e atualizado, assim como possuir a criptografia de disco rígido ativada.

Toda informação compartilhada com terceiros, deve ser realizada através da estrutura de equipes dentro da ferramenta Microsoft Teams, Sharepoint ou OneDrive.

4.9. Exceções

As diretrizes aqui descritas são consideradas como regulamento obrigatório na UY3 SOCIEDADE DE CRÉDITO DIRETO S.A. Exceções devem ser formalmente aprovadas pela Diretoria.

4.10. Processo Disciplinar

O não cumprimento a esta Política e as suas Normas, assim como a demais definições regulamentares e legais internas ou externas, por qualquer usuário, é passível de responsabilização cível ou penal, advertências por parte da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A e responsabilização prevista nas Leis do Trabalho, inclusive podendo ocorrer o desligamento por justa causa.

5. GOVERNANÇA E RESPONSABILIDADES

5.1. Gestores

Cumprir e fazer cumprir com as responsabilidades descritas neste documento atreladas aos instrumentos normativos que suportam as atividades inerentes ao seu setor, mantendo os padrões adotados pela Instituição, fazendo a revisão anual obrigatória, além das alterações necessárias para dar conformidade à legislação vigente.

5.2. Segurança da Informação

a) Estabelecer as melhores práticas de gestão;

b) Envolver as áreas da organização, visando manter um elevado nível de segurança para o atendimento dos requisitos de negócios;

c) Prover as discussões e alterações necessárias, visando manter o documento aderente as necessidades da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A.;

d) Fazer a gestão e garantir que as responsabilidades estabelecidas estão sendo cumpridas;

e) Prover manutenção a este documento;
f) Condução de testes periódicos de efetividade;
g) Gestão de riscos cibernéticos;
h) Elaboração do relatório anual de segurança cibernética.

5.3. Todas as demais áreas

a) Cumprir com as responsabilidades acordadas;

b) Propor alterações sempre que necessário.

5.4. Conselho de Administração e Diretoria

a) Aprovar esta política e suas revisões anuais;
b) Supervisionar os riscos cibernéticos;
c) Receber relatórios periódicos de riscos e incidentes relevantes;
d) Garantir recursos adequados para implementação dos controles.

6. GESTÃO DE RISCOS CIBERNÉTICOS

A UY3 SOCIEDADE DE CRÉDITO DIRETO S.A., manterá processo formal de:

- Identificação de ativos críticos;
- Avaliação de ameaças e vulnerabilidades;
- Classificação de riscos (impacto e probabilidade);
- Definição de plano de tratamento;
- Reporte periódico à Alta Administração (diretoria);
- Revisão mínima anual ou quando houver mudança relevante.

7. CONTROLES MÍNIMOS OBRIGATÓRIOS

7.1 Controle de Acesso e Autenticação

- Adoção obrigatória de autenticação multifator (MFA) para acessos privilegiados e ambientes críticos;
- Aplicação do princípio de menor privilégio;
- Revisão periódica de acessos a cada 06 meses;
- Segregação de funções.

7.2 Criptografia

- Criptografia de dados em trânsito e em repouso;
- Gestão segura de chaves criptográficas;
- Revogação imediata de chaves comprometidas;
- Proteção reforçada para chaves privadas utilizadas em assinatura digital.

7.3 Monitoramento Contínuo e SIEM

- Centralização de logs em solução de monitoramento (SIEM);
- Monitoramento contínuo de eventos de segurança;
- Correlação de eventos e geração de alertas;
- Retenção de registros por, no mínimo, 5 anos quando aplicável;
- Segregação de funções entre operação e monitoramento.

7.4 Gestão de Vulnerabilidades

- Varredura periódica de vulnerabilidades;
- Classificação por criticidade;
- SLA formal de correção, sendo crítico em até 30 dias e altas em até 60 dias ;
- Evidência documental das remediações.

7.5 Teste de Intrusão Independentes

- Realização de teste de intrusão anual;
- Execução por empresa ou profissional independente;
- Relatório técnico e executivo;
- Plano de ação formal aprovado pela Diretoria;
- Evidência de correção das vulnerabilidades identificadas.

7.6 Inteligência Cibernética

- Monitoramento de ameaças em internet pública, Deep Web e Dark Web;
- Monitoramento de vazamento de credenciais;
- Acompanhamento de indicadores de comprometimento;
- Uso de inteligência para prevenção e resposta a incidentes.

7.7 Segurança de APIs e Integrações

- Autenticação forte em APIs;
- Controle de acesso baseado em escopo;
- Monitoramento de chamadas e detecção de anomalias;
- Proteção contra abuso e ataques automatizados.

7.8 Proteção de Infraestruturas Críticas

- Isolamento lógico e/ou físico
  (transações PIX, liquidações STR e comunicação RSFN);
- Controle rigoroso de acesso;
- Validação de integridade antes de assinatura digital;
- Monitoramento reforçado de transações críticas.

7.9 Prevenção e Resposta a Incidentes

- Plano formal de Resposta a Incidentes;
- Comunicação imediata de incidentes relevantes à Diretoria;
- Registro detalhado de incidentes;
- Testes periódicos de simulação;
- Avaliação pós-incidente com lições aprendidas.

7.10 Backup e Continuidade

- Política formal de backup;
- Testes periódicos de restauração a cada 06 meses;
- Plano de Continuidade de Negócios;
- Garantia de resiliência operacional.

7.11 Gestão de Terceiros

- Avaliação prévia de risco cibernético;
- Cláusulas contratuais específicas de segurança;
- Monitoramento contínuo de fornecedores críticos;

- Inclusão de terceiros no escopo de segurança quando aplicável.

8. EVIDÊNCIAS E AUDITABILIDADE

A UY3 SOCIEDADE DE CRÉDITO DIRETO S.A. manterá documentação e evidências operacionais dos controles implementados, incluindo:

- Logs;
- Relatórios de pentest;
- Planos de ação;
- Relatórios de incidentes;
- Relatórios de riscos.

Todos os documentos permanecerão disponíveis para supervisão pelo regulador por prazo mínimo de 5 anos. E a efetividade dos controles será avaliada periodicamente por meio de testes independentes e auditorias internas.

9. RELATÓRIO ANUAL

Será elaborado o relatório anual, que será submetido à diretoria, contendo:

- Incidentes relevantes;
- Resultados de testes;
- Avaliação de riscos;
- Plano de melhorias.

Legislação e Normativos Aplicáveis

- Resolução CMN nº 5.274/2025
- Resolução CMN nº 4.893/2021
- Lei 13.709/2018 – Lei Geral de Proteção de Dados
- Lei dos Crimes Cibernéticos, Lei nº 12.737/2012
- ISO/IEC 27001/2013 - Sistema de Gestão da Segurança da Informação
- ISO/IEC 27002 Código de prática para controles de segurança da informação 2022
- Marco Civil da Internet, Lei nº 12.965/2014

TERMO DE ACEITE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

O Usuário infra-assinado declara ter recebido e lido a presente Política de Segurança da Informação da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A., estando ciente e concordando com as diretrizes, obrigações, deveres e recomendações nela previstas. Ainda, declara o usuário, estar ciente de que a Política de Segurança da Informação e Cibernética está disponível na Rede Interna, bem como pode ser solicitada através do e-mail seguranca@uy3.com.br.

Ainda, o usuário abaixo nominado, reconhece a legitimidade da UY3 SOCIEDADE DE CRÉDITO DIRETO S.A., para monitorar suas atividades laborativas, com a finalidade de manutenção da ordem e segurança pessoal de seus colaboradores, bem como da integridade da rede corporativa (informática e telefonia) e dos equipamentos e sistemas de sua propriedade, além do necessário sigilo das informações.

_____, _____ de _____ de _____.

_____

Assinatura