1. OBJETIVO

O presente documento tem por objetivo expressar o posicionamento da UY3 SOCIEDADE DE CREDITO DIRETO S.A. sobre os princípios e diretrizes que visam assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informações relacionadas à segurança cibernética em conformidade a resolução do BACEN 4.893/2021.

O desenvolvimento desta política realizou-se observando o porte, perfil de risco, modelo de negócio, natureza das operações e a complexidade dos produtos e serviços, sendo considerada uma extensão da **UY3-PO-TI-001 – Política de Segurança da Informação.**

2. AMBITO

Aplica-se a todo e qualquer ativo de informações e usuário com acesso às informações da UY3 SOCIEDADE DE CREDITO DIRETO S.A., independentemente de seu vínculo com a Instituição.

3. CONCEITO

3.1. Segurança da Informação

É o conjunto de conceitos que visa a preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, como autenticidade, responsabilidade, não-repúdio e confiabilidade.

3.2. Segurança Cibernética

É o conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas de TI e dados de ataques, danos ou acesso não autorizado.

3.3. Vulnerabilidade

É a fragilidade de um ativo ou grupo de ativos em ser explorado por uma ou mais ameaças internas ou externas.

3.4. Incidente

Traduz a ocorrência de uma ação que comprometeu a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite.

3.5. Riscos Cibernéticos

Identificados por ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor Dados, redes e sistemas da UY3 SOCIEDADE DE CREDITO DIRETO S.A., causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades.

3.6. Resiliência

É a capacidade do ativo ou ambiente de voltar ao seu estado original, posterior ao incidente ocorrido.

3.7. Usuário

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

3.8. Proprietário de Ativos

Uma pessoa ou entidade autorizada a controlar o uso e a segurança dos ativos, tornando-se o responsável por eles.

4. PREMISSAS

4.1. Monitoramento e Rastreabilidade

a) Avaliar se a causa da falha do controle foi identificada;
b) Validar se todo o ambiente conseguiu ter o seu retorno da forma esperada (resiliência);
c) Correlacionar as causas e os eventos para identificação futura e estabelecimento de lições aprendidas;
d) Determinar que o monitoramento é uma atividade interdepartamental;
e) Determinar qual foi o ambiente afetado pela falha do controle;
f) Determinar qual foi o controle que houve falha;
g) Determinar qual foi o tempo de retorno para o ambiente;
h) Determinar quais os métodos foram utilizados para sanar a exploração da falha;
i) Avaliar se existem resquícios de falhas de controle para o ambiente.

4.2. Gestão de Vulnerabilidades

Deve prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente, avaliando periodicamente as vulnerabilidades encontradas no ambiente corporativo.

4.3. Plano de Ação e Respostas a Incidentes

Comunicar um incidente ou suspeita dele assim que detectado ao seu superior imediato ou a segurança da informação através dos canais de e-mail, teams e sistema chamados.
Esta informação deve seguir o seguinte formato:

a) Identificação do incidente;
b) Área onde foi identificador do incidente;
c) Usuário identificador do incidente e seu contato;
d) Ativo onde ocorreu o Incidente;
e) Situação do Incidente;
f) Data do Incidente;
g) Nível de alerta do incidente;

h) Áreas envolvidas na investigação;

i) Correlação com outros incidentes.

j) Riscos identificados;

Observar as demais definições para a tomada de decisão/ação nos casos de incidentes de segurança da informação conforme a norma **UY3-PL-SI-001 – Plano de Ação e Respostas a Incidentes.**

4.4. Gestão de Risco Cibernético

A gestão de riscos deve possuir os seguintes princípios para identificação, avaliação, validação e tratamento de riscos apontado:

a) Identificador do Risco;

b) Avaliação de impacto/consequência;

c) Validação do impacto e da consequência do risco no ambiente;

d) Validação da frequência/probabilidade em que o risco acontece no ambiente;

e) Plano de Tratamento de Risco;

f) Comunicação de Risco;

g) Continuidade de Negócio;

4.5. Plano de Conscientização de Segurança da Informação

Na contratação de novos funcionários todos recebem o Termo de Uso Aceitável de Recursos de Informática assim como a Política de Segurança da Informação, devendo tomar ciência de seus respectivos conteúdos.

A política resumida de segurança da informação e cibernética para o público está disposta em nosso site www.uy3.com.br.

O plano de conscientização está disponível no plano **UY3-PL-SI-002 – Plano de Conscientização de Segurança da Informação.**

4.6. Proteção contra Softwares Maliciosos

a) Deve ser definido software para avaliação de ameaças internas;
b) Deve ser avaliado se a varredura online está ativa nas estações de trabalho e servidores em período razoável;
c) Deve ser registrado e comunicado qualquer incidente relacionado a códigos maliciosos;
d) As assinaturas contra ameaças devem estar atualizadas com a última versão do fabricante;

4.7. Prevenção de Vazamento de Dados

a) Deve ser utilizado a classificação da informação para estabelecer a correlação de eventos;
b) Todos os colaboradores, prestadores de serviço e/ou terceiros devem ter o conhecimento sobre os pontos informados da Política de Segurança da Informação e Política de Segurança Cibernética;
c) As informações devem estar rastreadas contendo marcadores;
d) Todos os dados devem estar classificados;
e) Os seguintes fluxos de saída de informação devem estar monitorados:
    - Webmail;
    - Ferramentas de comunicação instantâneas;
    - Servidores de transferência de informação;
    - Acesso de terceiros e prestadores de serviço.

4.8. Prevenção e Detecção de Intrusão

a) Todas as aplicações web que estão publicadas, devem possuir logs ativos e rastreabilidade de acesso;
b) Todas as aplicações web que estão publicadas, devem possuir ao menos ferramentas mínimas de segurança ativadas;
c) Todo ambiente que mantem aplicações deve apenas possuir os serviços necessários ativos;
d) Todas as aplicações devem estar em sua última atualização estável;
e) Todo tráfego entre cliente e a aplicação deve utilizar criptografia forte.

f) Toda aplicação deve possuir mecanismos de autenticação (usuário\senha) fortes.

g) É desejável que todas as aplicações tenham login único através do controlador de domínio do UY3 para usuários internos.

4.9. Autenticação

Todos os sistemas de informação devem possuir ao menos um fator de autenticação conforme definição abaixo:

a) Algo que o colaborador é: Digital, Iris;

b) Algo que o colaborador tem: Token de Acesso;

c) Algo que o colaborador conhece: Username, Password;

d) Onde o colaborador está: Certificado de máquina;

Os fatores acima devem ser instituídos de acordo com a criticidade dos acessos e a criticidade das informações acessadas. As senhas devem seguir requisitos mínimos de segurança (mínimo 8 caracteres, usar caracteres especiais "*$@#!%*", conter números e letras maiúsculas/minúsculas).

Acessos externos para fornecedores/terceiros devem possuir ao menos 2 fatores de autenticação.

4.10. Gerenciamento de Identidade e Acesso

Os colaboradores devem possuir perfis de acesso restrito, contendo as funções inerentes a atividades que necessitam (conceito de menor privilégio).

O controle de acesso deve ser utilizado de acordo com a criticidade dos acessos e a criticidade das informações acessadas. Em sistemas que contenham informações sensíveis, deve ser feito um perfil especial para a equipe de segurança da informação, auditoria/compliance para avaliação de eventos de segurança e auditoria de acessos. Somente usuários sistêmicos devem possuir acesso direto a base de dados e, com a possibilidade de auditar todos os comandos executados na plataforma. A periodicidade de alteração da senha e sua composição serão definidas pela área de segurança da informação.

Quando um colaborador for desligado da área de segurança ou tecnologia, que contenham acesso privilegiados, deve ser feito a alteração das senhas conhecidas por este.

A auditoria (accounting) de sistemas deve ocorrer anualmente ou quando necessário e, deve ser avaliado o perfil de acesso de colaboradores e as atividades que possam impactar ao ambiente.

4.11. Criptografia

Todos os sistemas que possuam plataforma WEB devem utilizar certificado de acesso (SSL) válido. O certificado deve ser constituído por uma autoridade certificadora confiável.

Somente algoritmos de criptografia aprovados pela área de segurança da informação devem ser utilizados nas soluções e sistemas adotados pela UY3. O gerenciamento das chaves de criptografia deve prever mecanismos para o armazenamento seguro, geração segura da chave e destruição da chave.

Caso seja comprometida uma chave criptográfica, deve ser revogada imediatamente. Se for uma chave para criptografia de arquivos, deve ser trocada. Mecanismos de autenticação e auditoria devem ser estabelecidos para garantir a segurança do acesso às chaves criptográficas.

As comunicações entre sistemas, que possuam informações sensíveis, devem ser feitas utilizando o túnel de criptografia e, sendo segmentado entre redes.

4.12. Segmentação de Rede

A segmentação de rede deve cumprir com o mandatário da classificação da informação e, a segmentação deve utilizar o conceito de dados seguros, utilizando Firewall de acesso e diferenciação de VLANs para cada ambiente, utilizando as melhores práticas e diferenciando os ambientes de Produção, Homologação, Pré-Produção e Desenvolvimento.

Empresas terceiras e prestadores de serviço que possuem contrato de criação de ambiente, devem apenas ter acesso ao ambiente de Desenvolvimento e Pré-Produção.

O ambiente de Homologação e Produção devem ser exclusivos de colaboradores da UY3. Exceções deverão ser aprovadas pela diretoria de TI e/ou comitê gestor de segurança da Informação.

4.13. Arquitetura, Novas tecnologias e Desenvolvimento Seguro

Utilizar as melhores práticas de mercado, tendo em vista:

a) Avaliar em tempo de execução a codificação de sistemas afim de mitigar os riscos ao ambiente do banco (testes DAST e SAST).
b) Manter a segregação de ambientes (desenvolvimento, homologação e produção).
c) Realizar testes de intrusão ao final da codificação afim de mitigar vulnerabilidades que não tenham sido observadas em seu desenvolvimento.

4.14. Classificação da Informação

A informação deve ser classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação, devendo ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a UY3.

A Classificação de Informação é de responsabilidade do proprietário do ativo, analisando-o criticamente a intervalos regulares, e assegurando que ele está atualizado e no nível apropriado.

Os usuários, ao término do contrato de trabalho ou de prestação de serviço, não podem se apropriar de informações classificadas como confidenciais que tenham sido usadas, criadas ou disponibilizadas para o seu controle.

4.15. Manutenção de cópia de Segurança de dados

A manutenção de cópia de Segurança de dados deve seguir os seguintes pontos:

a) Definir a classificação dos dados para estabelecimento de cópia de segurança de dados;
b) Definir o tempo de retenção dos dados utilizando a definição exigida pelo órgão regulatório;
c) Garantir que as políticas e controles de manutenção de cópias de segurança dos dados (Aplicações, Infraestrutura, banco de dados, servidores de arquivo, estações de trabalho, Mobile etc.) dos ambientes cibernéticos estejam em conformidade com as melhores práticas de mercado;

d) Os dados mais sensíveis e que, não possuem regulamentação definida, devem ser armazenados por 90 dias (logs/eventos no próprio sistema/aplicação) e, ser armazenados por 1 ano em fitas backup ou outro método utilizado.

4.16. Processamento e armazenamento de dados e de computação em nuvem

No processo de contratação de serviços relevantes para processamento e armazenamento de dados em nuvem, a empresa contratada deve seguir os requisitos da resolução 4.9893/2021 onde a UY3 assegura-se de um procedimento efetivo para aderência as regras em vigor.

Os requisitos são representados pelo documento **UY3-QU-SI-001 - Questionário de Segurança da Informação**.

4.17. Relatório Anual

Estabelecer o Relatório Anual contendo os principais eventos de segurança da informação e cibernéticos ocorridas na UY3. Este relatório contempla os seguintes eventos:

a) Incidentes, atividades de resposta a incidente e plano de ação relevantes ocorridos no período.
b) Resultados dos testes de Continuidade de Negócio.
c) Demais incidentes relevantes relacionados com o ambiente cibernético ocorridos no período.

É de responsabilidade da área de Segurança da Informação elaborar o relatório anual sobre os eventos citados.

Todos os documentos relacionados à segurança da informação mencionados pela norma BACEN 4.893/2021 devem ficar à disposição para consultas pelo prazo de cinco anos.

5. RESPONSABILIDADE

5.1. Conselho de Administração ou Diretoria

Apoiar e aprovar os documentos relacionados a segurança das informações da UY3:

a) Esta Política de Segurança Cibernética;
b) Plano de Ação e de Respostas a Incidentes;
c) Relatório Anual.

5.2. 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.

5.3. 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 do Banco;
d) Fazer a gestão e garantir que as responsabilidades estabelecidas estão sendo cumpridas.

5.4. Compliance

a) Cumprir com as responsabilidades acordadas;
b) Prover manutenção a este documento.

5.5. Todas as demais áreas

a) Cumprir com as responsabilidades acordadas;
b) Propor alterações sempre que necessário.

6. LEGISLAÇÃO E NORMATIVOS APLICÁVEIS

- Resolução BACEN CVM 4.983/2021
- Lei 13.709/2018 – Lei geral de Proteção de Dados
- ISO/IEC 27001/2013 - Sistema de Gestão da Segurança da Informação
- UY3-PO-SI-001 Política de Segurança da Informação
- UY3-QU-SI-001 Questionário de Segurança da Informação