1. OBJETIVO

1.1. O objetivo da **Política de Segurança Cibernética ("PSC")** da U4C é traçar diretrizes para estabelecimento da implementação de um ambiente tecnológico e informacional seguro, a partir de um padrão interno, simplificando a gestão da informação e das operações associadas, o que abrange a gestão das atividades de contratação de serviços de processamento e armazenamento de dados, bem como a computação em nuvem.

1.2. A **PSC** estabelece os princípios, conceitos, diretrizes, valores e práticas que serão seguidos para reduzir a vulnerabilidade da Instituição a incidentes.

2. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

2.1. Esta política baseia-se nos seguintes princípios:

- Confiabilidade
- Integridade
- Confidencialidade
- Disponibilidade
- Autenticidade
- Não-repúdio ou irretratabilidade

3. PROCEDIMENTOS E OS CONTROLES ADOTADOS PARA REDUZIR A VULNERABILIDADE A INCIDENTES

3.1. <u>GESTÃO DE VULNERABILIDADE</u>

- Será implementado um processo contínuo de identificação de vulnerabilidades em sistemas, redes, aplicativos e outros ativos digitais.
- Serão utilizadas ferramentas de análise de vulnerabilidades para escanear e identificar possíveis falhas de segurança.

3.2. <u>PLANO DE AÇÃO E RESPOSTA A INCIDENTES</u>

- Anualmente, será elaborado Relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes, tendo como data-base o dia 31 (trinta e um) de dezembro de cada ano, o qual será apresentado à Diretoria Executiva da companhia, para aprovação, até 31 (trinta e um) de março do ano seguinte ao da data-base, e que será executado pelo Diretor nomeado, e abordará:
  - ➔ A efetividade da implementação das ações desenvolvidas para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da **PSC**;
  - ➔ O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizadas na prevenção e na resposta a incidentes;

- ➔ Os incidentes relevantes relacionados com o ambiente cibernético, ocorridos no período.
- ➔ Os resultados dos testes de continuidade de negócios.

3.3. SENHAS DE USUÁRIOS

- Os usuários irão acessar a plataforma através de credenciais armazenadas no banco de dados, com criptografia em trânsito protegida por chaves SSL e login único.
- Serão implementadas regras de segurança para proteção de acesso por múltiplas tentativas, bloqueando o acesso do usuário que errar a senha por várias vezes em um curto período de tempo.

3.4. GESTÃO DE ACESSOS

- O acesso a dados e funcionalidades será estritamente controlado, seguindo o princípio do "mínimo privilégio".
- Controles de acesso serão avaliados pela área de segurança da informação de acordo com procedimento específico para garantir a segurança cibernética e a proteção de dados.

3.5. PROTEÇÃO CONTRA CÓDIGO MALICIOSO

- Todos os colaboradores e prestadores de serviços deverão aderir às práticas de segurança estabelecidas, relatando imediatamente qualquer atividade suspeita à equipe de segurança.

3.6. SEGURANÇA DE REDES

- Serão utilizadas camadas de proteção de rede para controle de tráfego e acessos internos, assim como canal seguro entre escritório e ambiente *Cloud*.
- Será utilizada a solução de antivírus corporativo para apoiar nos pilares de prevenção, detecção e monitoramento do parque de dispositivos utilizados pelos colaboradores.

3.7. CÓPIAS DE SEGURANÇA (*BACKUP*)

- Diariamente será realizado o *backup* das instâncias de banco de dados, no qual serão armazenadas na própria *Cloud* sendo os mesmos com criptografia em repouso.
- Atendendo a requisitos de compliance, o *backup* das informações produzidas pelos colaboradores será mantido por 10 anos, assim como *backups* de e-mails, documentos e demais arquivos.

3.8. ARMAZENAMENTO

- Todos os dados serão classificados de acordo com sua sensibilidade, importância e

requisitos legais.

- Os dados serão armazenados em locais apropriados, considerando requisitos de segurança e acesso.

3.9. CRIPTOGRAFIA E GERENCIAMENTO DE CHAVES

- A comunicação entre camadas de *frontend* e APIs será criptografada com certificado SSL (criptografia em trânsito).
- Todas as senhas armazenadas, serão criptografadas no banco de dados.
- Chaves de acesso de API serão armazenadas em repositório na nuvem com acesso restrito pela área de segurança e infraestrutura.

3.10. UTILIZAÇÃO DOS ATIVOS DE TECNOLOGIA DA INFORMAÇÃO:

- **Responsabilidade pelo uso dos ativos**
  - ➔ O usuário autorizado será totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, não podendo utilizá-las para finalidade diversa, assim como pelas ações decorrentes da utilização, devendo agir com a máxima transparência e seriedade.
  - ➔ Todos os usuários seguirão o guia de recomendações e boas práticas básicas adotadas e divulgadas periodicamente pela área de segurança da informação.

3.11. GESTÃO DA MUDANÇA

- Mudanças serão consideradas como alterações planejadas em *hardware*, *software*, redes, configurações e procedimentos relacionados à Tecnologia da Informação.
- Toda mudança será submetida a um processo formal de solicitação, que inclui a descrição detalhada da alteração proposta, seus objetivos, impactos e um plano de implementação.

3.12. GESTÃO DA CONTINUIDADE DE NEGÓCIOS

- Será desenvolvido Plano de Continuidade de Negócios (PCN) o qual descreverá detalhadamente os procedimentos específicos que deverão ser seguidos por cada área, para a retomada de operações em caso de interrupções críticas.

3.13. TREINAMENTO E CONSCIENTIZAÇÃO

- Todos os novos colaboradores e prestadores de serviços passarão por um treinamento inicial abordando os princípios básicos de segurança cibernética, políticas da empresa e práticas recomendadas.
- Serão ministrados treinamentos regulares para atualização dos colaboradores e prestadores de serviços quanto às últimas ameaças cibernéticas, técnicas de

ataque e práticas de segurança relevantes.

3.14. DESENVOLVIMENTO SEGURO E SEGURANÇA NAS APLICAÇÕES

- Todo o código criado seguirá as melhores práticas de desenvolvimento seguro, incluindo a validação adequada de entrada, a prevenção de injeção de código, e a gestão correta de sessões.

3.15. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

- Antes de iniciar qualquer projeto de aquisição ou desenvolvimento, será realizada uma avaliação detalhada acerca das necessidades do negócio para garantir a adequação do sistema com as metas e objetivos da organização.

3.16. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS (*CLOUD*)

- Antes de contratar serviços em nuvem, será realizada uma avaliação das necessidades específicas da empresa, considerando requisitos de desempenho, segurança, conformidade e custo.

3.17. REGISTRO E MONITORAMENTO

- Os registros de eventos serão armazenados de maneira segura e acessível apenas por pessoal autorizado.
- Serão definidos diferentes níveis de registro, considerando a criticidade e sensibilidade das operações, permitindo um controle mais preciso das atividades.

3.18. AVALIAÇÃO PERIÓDICA

- Serão conduzidas avaliações de segurança da informação periodicamente, de acordo com cronograma definido pela equipe de segurança cibernética.

4. CONTROLES DE RASTREABILIDADE DA INFORMAÇÃO

4.1. Todas as informações serão identificadas e classificadas de acordo com sua sensibilidade e importância para a organização.

4.2. Será implementado um sistema de registro de acessos para monitorar quem, quando e por que acessou informações sensíveis.

4.3. Os registros de acesso serão mantidos por um período adequado de acordo com regulamentações e políticas internas.

5. INCIDENTES RELEVANTES

5.1. REGISTRO

- Os incidentes relevantes em segurança cibernética incluem, mas não se limitam a, violações de dados significativas, ataques avançados, comprometimento de sistemas críticos e eventos que possam ter impacto significativo nas operações e

reputação da empresa.

- A gravidade dos incidentes será avaliada com base no impacto nos sistemas, dados, confidencialidade, integridade, disponibilidade e conformidade.
- Um processo será implementado para identificar e classificar incidentes logo que detectados.

5.2. ANÁLISE DA CAUSA E DO IMPACTO

- Será estabelecido um *Incident Response Team* (IRT) composto por membros qualificados de diversas áreas, incluindo segurança cibernética, tecnologia da informação, comunicação e jurídico.
- A equipe de resposta a incidentes tomará medidas imediatas para conter e mitigar os incidentes relevantes, visando limitar danos e interrupções.
- Serão criados e seguidos procedimentos claros e testados para garantir uma resposta rápida e eficiente.
- Após a contenção, será conduzida uma investigação aprofundada para entender a origem, escopo e métodos do incidente.

5.3. CONTROLE DOS EFEITOS

- Logo que identificado o incidente, o Plano de continuidade de negócios será acionado conforme necessário, para minimizar o tempo de inatividade.
- Os incidentes relevantes serão notificados às autoridades competentes de acordo com regulamentações locais e internacionais.

6. DIRETRIZES

6.1. CENÁRIOS DE INCIDENTES CONSIDERADOS NOS TESTES DE CONTINUIDADE DOS SERVIÇOS

Os testes de continuidade dos serviços são fundamentais para garantir a resiliência e a capacidade de recuperação dos sistemas e processos essenciais. Diversos cenários de incidentes serão considerados durante esses testes para simular situações reais e verificar a eficácia dos planos de continuidade. Abaixo estão alguns exemplos de cenários de incidentes que podem ser contemplados nos testes de continuidade dos serviços:

- Incidentes de Segurança Cibernética:
- Ataques de denegação de serviço (DDoS):
- Erros humanos e falhas operacionais:
- Perda de conectividade:

6.2. PROCEDIMENTOS E CONTROLES VOLTADOS À PREVENÇÃO E AO TRATAMENTO DOS

INCIDENTES A SEREM ADOTADOS POR EMPRESAS PRESTADORAS DE SERVIÇOS QUE MANUSEIEM DADOS OU INFORMAÇÕES SENSÍVEIS OU QUE SEJAM RELEVANTES

Empresas prestadoras de serviço que eventualmente tenham acesso a manusear dados ou informações sensíveis estão sujeitas às regras definidas em procedimentos definidos pela área de segurança da informação e detalhados em contratos entre as partes.

6.3. CLASSIFICAÇÃO DAS INFORMAÇÕES E DOS DADOS PESSOAIS

- As informações serão classificadas com base em sua utilização da seguinte maneira:
  - ➔ Informação Pública
  - ➔ Informação Interna
  - ➔ Informação Confidencial
- Recomendações para a classificação dos dados:
  - ➔ Dados Pessoais Sensíveis
  - ➔ Dados Pessoais Não Sensíveis

6.4. DEFINIÇÃO DOS PARÂMETROS A SEREM UTILIZADOS NA AVALIAÇÃO DA RELEVÂNCIA DOS INCIDENTES

Todas as análises de eventos deverão ser suportadas por classificação de acordo com o impacto esperado, considerando o seguinte:

- Alto (Impacto Grave)
- Médio (Impacto Significativo)
- Baixo (Impacto Mínimo)

7. DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

7.1. PROGRAMAS DE CAPACITAÇÃO E DE AVALIAÇÃO PERIÓDICA DE PESSOAL

O programa de capacitação em segurança da informação tem como objetivo conscientizar e capacitar os colaboradores da U4C sobre as melhores práticas e políticas de segurança cibernética. Componentes do Programa:

- Treinamento Inicial
- Treinamentos Periódicos
- Simulações de *Phishing*
- Workshops Específicos

7.2. INFORMAÇÕES A USUÁRIOS FINAIS SOBRE PRECAUÇÕES NA UTILIZAÇÃO DE PRODUTOS E SERVIÇOS OFERECIDOS

- Antes do uso de um produto ou serviço, os usuários serão informados sobre quaisquer riscos associados.
- As precauções necessárias para mitigar esses riscos serão destacadas de maneira proeminente nas comunicações.
- Sempre que houver atualizações nos produtos ou serviços que impactem as precauções necessárias, os usuários serão prontamente informados.

7.3. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A Diretoria da U4C Instituição de Pagamento S.A. firma um compromisso com a melhoria contínua dos procedimentos relacionados com a segurança cibernética, buscando sempre se manter em conformidade com as normas e regulamentos aplicáveis, sob obediência ao princípios, diretrizes e práticas aqui adotadas para assegurar a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas de informação por ela utilizados.

8. INICIATIVAS PARA COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES RELEVANTES

8.1. Avaliação da relevância com base na potencial gravidade do incidente e seu impacto nos processos e nas partes interessadas, considerando que incidentes relevantes incluem qualquer evento que possa comprometer a segurança da informação, a continuidade operacional ou a confidencialidade de dados na U4C Instituição de Pagamento S.A..

8.2. Compartilhamento interno de informações sobre incidentes relevantes imediatamente com as partes-chave, incluindo a equipe de segurança da informação, gerência sênior e outros departamentos afetados.

8.3. Em casos em que a legislação exige ou quando a gravidade do incidente justifica, promover o compartilhamento de informações relevantes externamente com autoridades reguladoras, parceiros comerciais afetados e clientes, seguindo os protocolos legais e regulatórios aplicáveis.

9. ATRIBUIÇÕES E RESPONSABILIDADES

9.1. A equipe de segurança cibernética é responsável por monitorar, avaliar e responder a ameaças de segurança.

9.2. Todos os funcionários são responsáveis por seguir as práticas de segurança cibernética, relatar incidentes e participar de treinamentos regulares de conscientização.

9.3. A alta administração é responsável por alocar recursos adequados, revisar e aprovar políticas de segurança e garantir a conformidade com as regulamentações do BACEN.