	<p>POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO</p>	<p>Emissão 14/10/2024</p>	<p>Classificação Uso interno</p>
<p>Código N-SI-001</p>		<p>Versão 1.01</p>	<p>Aprovado por: P!nk Corp Administration.</p>

1. Introdução

- 1.1. A P!NK CORP é especializada em oferecer soluções de cartões de benefícios corporativos para outras empresas. Reconhecemos que a informação corporativa e pessoal é um ativo essencial para a continuidade e segurança das operações, além de garantir a proteção dos dados de nossos clientes e parceiros. A Política Geral de Segurança da Informação visa estabelecer uma gestão eficiente da segurança dos ativos e informações da organização, protegendo-os contra ameaças internas e externas.

2. Propósito

- 2.1. Estabelecer diretrizes de segurança que permitam o uso adequado das informações e recursos computacionais da P!NK CORP atendendo às necessidades de segurança de nossos clientes e parceiros;
- 2.2. Fornecer um ambiente seguro para o tráfego e armazenamento de dados relacionados aos contratos de cartões de benefícios, mantendo a integridade, confidencialidade e disponibilidade das informações;
- 2.3. Prevenir incidentes que possam impactar as operações, proteger a reputação da P!NK CORP e mitigar riscos financeiros e legais.

3. Escopo

- 3.1. Esta política aplica-se a todos os colaboradores, prestadores de serviço, e outros indivíduos com acesso às informações e recursos computacionais da P!NK CORP. A adesão a esta política é obrigatória, independentemente da natureza do vínculo com a organização.

4. Diretrizes

4.1. Gestão da Segurança da Informação

- 4.1.1. A P!NK CORP compromete-se a manter uma gestão efetiva da segurança da informação, suportando operações críticas e minimizando riscos para o negócio;

4.2. Classificação da Informação

- 4.2.1. Todas as informações são classificadas de acordo com seu nível de sensibilidade e criticidade, como Pública, Restrita e Confidencial. Essa classificação orienta as práticas de armazenamento e acesso aos dados.

	<p>POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO</p>	<p>Emissão 14/10/2024</p>	<p>Classificação Uso interno</p>
<p>Código N-SI-001</p>		<p>Versão 1.01</p>	<p>Aprovado por: P!nk Corp Administration.</p>

4.3. Implementação de Controles de Segurança

4.3.1. Serão implementados controles para garantir a confidencialidade, integridade e disponibilidade das informações, mitigando ameaças internas e externas e aderindo às melhores práticas e normas de segurança;

4.3.2. Controle de Acessos e Autenticação

4.3.2.1. São implementados mecanismos de autenticação forte e gestão de acessos baseados nas funções dos usuários, de forma a garantir que cada colaborador acesse apenas as informações necessárias para sua função.

4.4. Educação e Conscientização

4.4.1. Programas de conscientização serão disponibilizados a todos os colaboradores e contratados para garantir o entendimento e a adesão aos princípios de segurança da informação da P!NK CORP;

4.5. Conformidade com Leis e Regulamentos

4.5.1. A P!NK CORP assegura que todas as atividades estarão em conformidade com as regulamentações, leis e cláusulas contratuais aplicáveis à segurança da informação;


4.5.2. Privacidade e Conformidade com Legislações

4.5.2.1. Todas as operações de tratamento de dados pessoais são realizadas em conformidade com a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações, reforçando o compromisso com a privacidade.

4.6. Gestão de Incidentes de Segurança da Informação

4.6.1. Todos os incidentes serão devidamente registrados, investigados e corrigidos, e, se necessário, reportados às autoridades competentes;

4.6.2. Gestão de Riscos de Segurança da Informação

	<p align="center">POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO</p>	<p align="center">Emissão 14/10/2024</p>	<p align="center">Classificação Uso interno</p>
<p align="center">Código N-SI-001</p>		<p align="center">Versão 1.01</p>	<p align="center">Aprovado por: P!nk Corp Administration.</p>

4.6.2.1. A organização realiza avaliações periódicas de riscos e implementa medidas de mitigação para reduzir o impacto de potenciais incidentes de segurança, protegendo as informações sensíveis;

4.7. Continuidade de Negócios

4.7.1. Planos de continuidade e recuperação de desastres serão mantidos e aprimorados continuamente para garantir a resiliência das operações.

5. Papéis e Responsabilidades

5.1. Comitê de Segurança da Informação (CSI):

5.1.1. Responsável por analisar, aprovar e garantir os recursos necessários para uma gestão eficaz da segurança da informação. O CSI promoverá a disseminação da cultura de segurança e revisará periodicamente as políticas para adequação às necessidades da P!NK CORP;

5.2. Gerência de Segurança da Informação:

5.2.1. Responsável pela execução e operação da segurança da informação, apoiando o CSI e garantindo o cumprimento das normas e procedimentos;

5.3. Gestores de Informação:

5.3.1. Devem gerenciar e classificar adequadamente as informações sob sua responsabilidade, revisando periodicamente o acesso a essas informações;

5.4. Responsável pelo Tratamento de Dados Pessoais (DPO):

5.4.1. O DPO coordena as práticas de proteção de dados pessoais, assegurando a conformidade com a LGPD e agindo como ponto de contato com autoridades reguladoras e titulares dos dados;

5.5. Usuários da Informação:

5.5.1. Devem compreender e aderir integralmente às políticas e comunicar qualquer situação que possa representar um risco à segurança da informação;

	<p align="center">POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO</p>	<p align="center">Emissão 14/10/2024</p>	<p align="center">Classificação Uso interno</p>
<p align="center">Código N-SI-001</p>		<p align="center">Versão 1.01</p>	<p align="center">Aprovado por: P!nk Corp Administration.</p>

5.6. Auditoria Interna:

5.6.1. A auditoria realiza verificações periódicas para avaliar a eficácia dos controles de segurança e verificar a conformidade das práticas com as políticas de segurança da informação.

6. Sanções e Punições

6.1. A violação desta política estará sujeita a sanções que podem incluir advertências, suspensão e até demissão. No caso de terceiros, o contrato poderá ser encerrado e outras sanções aplicadas conforme os termos contratuais;

6.1.1. Advertência Verbal ou Escrita

6.1.1.1. Pequenas violações das políticas de segurança podem resultar em advertências, conforme avaliação do CSI e do departamento de recursos humanos;

6.1.2. Suspensão e Encerramento de Contrato

6.1.2.1. Violações graves ou reincidentes podem levar à suspensão do colaborador ou ao encerramento do contrato de trabalho ou prestação de serviços;

6.1.3. Responsabilização Legal


6.1.3.1. Para violações que envolvem atividades ilegais, a empresa poderá tomar as medidas legais cabíveis, responsabilizando o infrator por danos causados à organização e aos clientes;

6.1.4. Rescisão Contratual para Terceiros

6.1.4.1. No caso de parceiros e prestadores de serviço, violações graves da segurança podem resultar na rescisão contratual, sendo assegurada a comunicação às partes envolvidas;

6.1.5. Escalonamento de Sanções

6.1.5.1. O CSI aplicará as sanções de forma escalonada, considerando a gravidade, frequência e o impacto da violação, conforme estipulado em um processo disciplinar formal.

	<p>POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO</p>	<p>Emissão 14/10/2024</p>	<p>Classificação Uso interno</p>
<p>Código N-SI-001</p>		<p>Versão 1.01</p>	<p>Aprovado por: P!nk Corp Administration.</p>

7. Revisões

- 7.1. Esta política será revisada anualmente pelo CSI para garantir sua adequação às mudanças tecnológicas e às necessidades da P!NK CORP.

7.1.1. Revisão Anual

- 7.1.1.1. A política de segurança da informação será revisada anualmente para manter-se atualizada com as práticas do mercado e os requisitos de conformidade;

7.1.2. Revisão Adicional em Caso de Incidentes Relevantes

- 7.1.2.1. Após incidentes significativos, o CSI fará uma análise e, se necessário, atualizará a política para evitar recorrências;

7.1.3. Avaliação por Consultorias Externas

- 7.1.3.1. Consultorias especializadas podem ser contratadas para revisar a política e os processos de segurança, promovendo a adoção de melhorias contínuas;

7.1.4. Feedback de Colaboradores e Clientes

- 7.1.4.1. Comentários e sugestões dos colaboradores e clientes sobre as políticas de segurança serão considerados em revisões anuais para assegurar a adaptabilidade das normas;

7.1.5. Planejamento de Mudanças Organizacionais

- 7.1.5.1. Mudanças internas, como fusões, aquisições ou expansão de serviços, serão acompanhadas de revisões na política para adaptação ao novo contexto organizacional;

8. Gestão da Política

- 8.1. A Política Geral de Segurança da Informação é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da P!NK CORP.

- 8.2. A presente política foi aprovada no dia 14/10/2024