	<b>RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</b>	Emissão <b>14/10/2024</b>	Classificação <b>Uso interno</b>
		Versão <b>1.03</b>	Aprovado por: <b>P!nk Corp Administration.</b>

## 1. Introdução

- 1.1. Esta Norma de Resposta a Incidentes de Segurança da Informação complementa a Política Geral de Segurança da Informação da P!NK CORP, que oferece soluções de cartões de benefícios corporativos para outras empresas. Esta norma estabelece diretrizes para a resposta e o tratamento de incidentes que possam comprometer a integridade, confidencialidade e disponibilidade dos ativos de informação e recursos computacionais.

## 2. Propósito

- 2.1. O propósito desta norma é assegurar que todos os incidentes de segurança da informação sejam identificados, classificados e tratados de maneira adequada, minimizando o impacto nos serviços e garantindo a restauração das operações com segurança.

## 3. Escopo

- 3.1. Esta norma aplica-se a todos os ativos e serviços de informação, colaboradores, parceiros e terceiros que interajam com os recursos computacionais e sistemas da P!NK CORP.


## 4. Diretrizes

### 4.1. Identificação e Classificação de Incidentes de Segurança

- 4.1.1. Todos os eventos que possam comprometer a segurança dos dados e serviços da P!NK CORP devem ser identificados como incidentes de segurança e classificados com base na criticidade dos ativos afetados e na gravidade do impacto potencial;

### 4.2. Priorização e Comunicação de Incidentes

- 4.2.1. Incidentes de segurança serão priorizados considerando o nível de criticidade e o impacto estimado. Todos os incidentes devem ser reportados imediatamente à área de segurança da informação, que determinará a criticidade e, se necessário, notificará o Time de Resposta a Incidentes e as partes interessadas;

	<b>RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</b>	<b>Emissão</b> 14/10/2024	<b>Classificação</b> Uso interno
		<b>Versão</b> 1.03	<b>Aprovado por:</b> P!nk Corp Administration.

#### 4.3. Isolamento e Contenção

- 4.3.1. Qualquer ativo ou serviço com suspeita de comprometimento deve ser isolado do ambiente corporativo para conter a propagação do incidente, protegendo a integridade dos sistemas e informações;

#### 4.4. Análise de Impacto e Definição de Ações de Remediação

- 4.4.1. A extensão dos danos causados pelo incidente será analisada para determinar o melhor curso de ação para a eliminação completa da ameaça e recuperação dos ativos afetados;

#### 4.5. Eliminação e Recuperação

- 4.5.1. Após a eliminação do incidente, os ativos e serviços de informação serão restaurados ao seu estado de funcionamento normal, adotando medidas para garantir que a ameaça foi removida completamente e que o incidente não possa se repetir;


#### 4.6. Análise Pós-Incidente e Adoção de Melhorias

- 4.6.1. Uma revisão completa será realizada após o incidente, documentando o impacto, as vulnerabilidades exploradas, a eficácia das respostas aplicadas e as ações de melhoria que possam ser adotadas para fortalecer as defesas de segurança da P!NK CORP.

### 5. Time de Resposta a Incidentes de Segurança da Informação

#### 5.1. Composição do Time de Resposta

- 5.1.1. O Time de Resposta a Incidentes deve incluir representantes das áreas de Tecnologia da Informação, Segurança da Informação, Recursos Humanos e Jurídico. Em casos de incidentes específicos, outros colaboradores poderão ser convocados conforme necessário;

	<b>RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</b>	<b>Emissão</b> 14/10/2024	<b>Classificação</b> Uso interno
		<b>Versão</b> 1.03	<b>Aprovado por:</b> P!nk Corp Administration.

## 5.2. Responsabilidades do Time de Resposta

5.2.1. O Time de Resposta deve apoiar a Gerência de Segurança na identificação, contenção e eliminação de incidentes. Além disso, deve fornecer orientações estratégicas sobre o incidente, incluindo conselhos para a comunicação com as partes interessadas e a tomada de decisões estratégicas;

## 5.3. Disseminação de Informações sobre Incidentes

### 5.3.1. Confidencialidade das Informações sobre Incidentes

5.3.1.1. Nenhuma informação sobre incidentes de segurança poderá ser divulgada para pessoas ou entidades externas à P!NK CORP sem a aprovação formal da diretoria;

### 5.3.2. Aprovação de Comunicações Internas e Externas

5.3.2.1. Toda comunicação relacionada a incidentes de segurança será aprovada pela Gerência de Comunicação antes da divulgação, assegurando a consistência e a confidencialidade das informações;

## 6. Sanções e Punições

6.1. A violação das diretrizes e práticas estabelecidas pela Norma de Resposta a Incidentes de Segurança da Informação será tratada de forma rigorosa, conforme o nível de impacto e gravidade do incidente. As sanções visam reforçar a responsabilidade dos colaboradores e terceiros no cumprimento das políticas de segurança da P!NK CORP.


### 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. Rescisão Contratual com Justa Causa

	<b>RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</b>	<b>Emissão</b> 14/10/2024	<b>Classificação</b> <b>Uso interno</b>
<b>Código</b> N-SI-010		<b>Versão</b> 1.03	<b>Aprovado por:</b> <b>P!nk Corp</b> <b>Administration.</b>

6.1.3.1. Para violações graves e intencionais, que comprometam severamente a segurança da P!NK CORP ou os dados dos clientes, a empresa poderá rescindir o contrato de trabalho ou de prestação de serviço com justa causa. Esse tipo de sanção é aplicado a infrações que resultaram em danos financeiros ou reputacionais significativos;

#### 6.1.4. **Rescisão Contratual para Terceiros e Prestadores de Serviço**

6.1.4.1. Para fornecedores e terceiros que violem as políticas de segurança de forma grave, ou que se recusem a cooperar na resposta a incidentes, o contrato poderá ser rescindido imediatamente. A P!NK CORP reserva-se o direito de buscar ressarcimento por quaisquer danos causados pela violação;

#### 6.1.5. **Responsabilização Legal e Busca de Reparação por Danos**

6.1.5.1. Quando a violação das normas resultar em atividades ilegais, como a divulgação de informações confidenciais ou o acesso não autorizado a sistemas de dados protegidos, a empresa poderá tomar medidas legais contra o responsável. Isso inclui ações judiciais para a recuperação de prejuízos financeiros e danos à imagem da empresa;

#### 6.1.6. **Escalonamento de Sanções**


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

#### 6.1.7. **Participação Obrigatória em Treinamento de Segurança**

6.1.7.1. Colaboradores e terceiros que cometerem infrações menos graves, mas que demonstraram desconhecimento das normas, poderão ser obrigados a participar de treinamentos adicionais sobre segurança da informação. Esse treinamento visa corrigir falhas e garantir maior conscientização para prevenir futuros incidentes.

## 7. **Revisões**

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação;

	<b>RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</b>	<b>Emissão</b> 14/10/2024	<b>Classificação</b> Uso interno
<b>Código</b> N-SI-010		<b>Versão</b> 1.03	<b>Aprovado por:</b> P!nk Corp Administration.

## 8. Gestão da Norma

- 8.1. A norma **N-SI-010** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da P!NK CORP.
- 8.2. A presente norma foi aprovada no dia 14/10/2024