P!NK CORP	PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS	Emissão 14/10/2024	Classificação Uso interno
Código N-SI-006		Versão 1.03	Aprovado por: P!nk Corp Administration.

1. Introdução

1.1. A Norma de Proteção Contra Códigos Maliciosos complementa a Política Geral de Segurança da Informação da P!NK CORP, especializada em soluções de cartões de benefícios corporativos para outras empresas. Esta norma define diretrizes para a proteção dos sistemas, dados e ativos de informação contra ameaças de códigos maliciosos (malware) que possam comprometer a segurança e a continuidade das operações.

2. Propósito

2.1. Estabelecer diretrizes para a proteção eficaz dos ativos de informação da P!NK CORP contra códigos maliciosos, prevenindo infecções e garantindo a segurança dos sistemas e dados corporativos.

3. Escopo

3.1. Esta norma aplica-se a todos os usuários e dispositivos (computadores, dispositivos móveis e servidores) que acessem ou manuseiem informações da P!NK CORP.

4. Diretrizes

4.1. Ferramentas de Proteção Contra Códigos Maliciosos

4.1.1. **Soluções de Segurança Corporativas**: A P!NK CORP disponibiliza ferramentas específicas para proteção contra ameaças como vírus, trojans, worms e spyware. Essas ferramentas são obrigatórias em todas as estações de trabalho, dispositivos móveis e servidores;

4.1.2. **Uso Exclusivo de Ferramentas Autorizadas**: Apenas as ferramentas de proteção fornecidas pela P!NK CORP devem ser usadas para defesa contra códigos maliciosos. Ferramentas de terceiros não autorizadas são proibidas.

4.1.3. **Atualizações e Escaneamento**: As ferramentas de proteção contra malware devem:

4.1.3.1. Atualizar automaticamente suas assinaturas de malware em tempo real;

4.1.3.2. Realizar varreduras diárias em todos os arquivos nas unidades de armazenamento;

4.1.3.3. Em servidores, as varreduras podem ser restritas a pastas e arquivos críticos para evitar impactos no desempenho.

4.1.4. **Bloqueio de Ameaças**: Sites, arquivos e serviços suspeitos ou detectados como maliciosos serão bloqueados automaticamente para prevenir infecções.

4.2. **Isolamento em Caso de Infecção Suspeita**

4.2.1. **Dispositivos de Usuário**: Qualquer dispositivo suspeito de infecção deve ser imediatamente desconectado da rede corporativa e da internet para contenção;

4.2.2. **Servidores Corporativos**: Em caso de infecção suspeita em servidores, medidas de isolamento devem ser tomadas de forma a minimizar o impacto e proteger os serviços críticos da P!NK CORP.

4.3. **Prevenção e Boas Práticas para Usuários**

4.3.1. **Proibição de Correções Próprias**: Usuários não devem tentar corrigir infecções de malware por conta própria. Toda suspeita de infecção deve ser reportada imediatamente ao departamento de TI;

4.3.2. **Cuidados com Arquivos**: Arquivos recebidos por e-mail, baixados da internet ou em dispositivos removíveis devem ser escaneados com as ferramentas corporativas antes de seu uso;

4.3.3. **MACROS e Arquivos Suspeitos**: É proibido habilitar MACROS em documentos de origem desconhecida ou suspeita. A equipe de Segurança da Informação deve ser consultada para validação.

5. Papéis e Responsabilidades

5.1. **Gerência de Tecnologia da Informação**

5.1.1. Responsável por tratar infecções ou suspeitas de infecção por malware, notificando a equipe de Segurança da Informação quando necessário para avaliação adicional;

5.2. **Gerência de Segurança da Informação:**

5.2.1. Responsável por garantir que novas ameaças e variantes de malware sejam rapidamente identificadas e tratadas. É também responsável por divulgar orientações de segurança e informações sobre novas ameaças para os usuários;

6. Sanções e Punições

6.1. Violações das diretrizes desta norma, incluindo o uso não autorizado de softwares de proteção ou a negligência em seguir as práticas de segurança, estão sujeitas a sanções conforme a Política Geral de Segurança da Informação. As penalidades incluem advertências, suspensão e rescisão de contrato, dependendo da gravidade da infração.

7. Revisões

7.1. Esta norma será revisada anualmente, ou sempre que o Comitê Gestor de Segurança da Informação considerar necessário, para garantir a sua conformidade com as melhores práticas e a evolução das ameaças digitais.

8. Gestão da Norma

8.1. A norma **N-SI-006** 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