POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

SUMÁRIO

1. OBJETIVO

A Política Pública de Segurança da Informação e Cibernética ("Política") define um conjunto de princípios, diretrizes e responsabilidades, que conduzem as atividades pertinentes à prevenção e controle dos riscos, em linha com as melhores práticas de mercado, considerando-se a natureza e a complexidade dos produtos, serviços, atividades processos, sistemas e em conformidade com a legislação aplicável e requerimentos regulatórios em vigência.

2. ABRANGÊNCIA

A política abrange os principais aspectos do gerenciamento dos riscos relacionados aos eventos de Segurança da Informação e Cibernética que possam ocorrer nas rotinas diárias relacionadas aos ativos de informação, produtos, negócios, serviços prestados ou contratados.

Aplica-se às empresas do Conglomerado Prudencial Omni assim como aos seus administradores, colaboradores e prestadores de serviços terceirizados.

3. DIRETRIZES

3.1. Treinamento e Conscientização

Todos os colaboradores devem participar e apoiar o treinamento de segurança e requisitos de conscientização da organização.

3.2. Cooperação entre Organizações

Devem ser estabelecidos e mantidos contatos com as autoridades de segurança pública, órgãos reguladores e grupos de segurança, para prestação de contas e compartilhamento de conhecimento e assistência com incidentes de segurança, conforme apropriado.

3.3. Gestão de Ativos

Todos os colaboradores e prestadores de serviços devem cumprir as diretrizes de uso aceitável dos ativos estabelecidas em norma.

3.4. Classificação da Informação

Toda informação deve ter um responsável principal e uma classificação atribuída com base em diretrizes internas normatizadas. Todo tratamento das informações deverá seguir 4 procedimentos baseados na respectiva classificação de modo que possam garantir a confidencialidade, integridade e disponibilidade.

3.5. Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Instituição, para que sejam recomendadas as proteções adequadas.

3.6. Gerenciamento de Vulnerabilidades

Devem ser realizados, periodicamente, análises e testes de vulnerabilidades nos principais ativos conforme critérios internos e as boas práticas de mercado. Deve existir uma governança sobre os resultados de modo a avaliar riscos e priorizar correções considerando os principais vetores de criticidade, explorabilidade e impacto nos negócios.

3.7. Gerenciamento de Operações

3.7.1. Registro e Monitoramento de Eventos

Deve manter um processo de captura e monitoramento de informações relacionadas à interação entre os colaboradores e ativos de informação.

3.7.2. Gerenciamento de Incidentes de Segurança

Devem ser estabelecidos processos para detectar, registrar, classificar, tratar e reportar eventos relacionados a incidentes que possam afetar os pilares da segurança da informação.

3.7.3. Software de Antivírus e Código Malicioso
Os controles de detecção e prevenção contra software de código malicioso e vírus devem existir em todos os ativos de informação da organização.

3.7.4. Backup e Retenção
Deve existir a execução de backups periódicos dos ativos de informação, para propósitos de recuperação operacional. Os backups devem ser retidos, de acordo com requisitos de negócios e regulatórios.

Os procedimentos de restauração da informação devem ser testados em intervalos regulares.

3.7.5. Controles criptográficos
O grau de sensibilidade, baseado na classificação da informação, deve ser preservado através de criptografia.

3.7.6. Segurança de Rede
O acesso às transmissões de dados, bem como controlar o fluxo de dados entre as redes internas e públicas externas, devem ser limitados através do uso de soluções de segurança e monitoramento contínuo.

3.7.7. Gestão de Acessos
Devem ser estabelecidas diretrizes para gestão de acessos ao ambiente tecnológico, sistemas, plataformas ou ferramentas.

A administração de acesso deve utilizar ferramentas e processos rastreáveis. A identificação deve ser única, pessoal e intransferível.

3.8. Segregação de funções
As funções e responsabilidades incompatíveis devem ser segregadas de modo a minimizar conflitos de interesses, uso indevido ou não autorizado de informações da organização.

3.9. Segregação de ambientes

Os ambientes produtivos e não-produtivos devem ser segregados para minimizar a possibilidade de modificações não autorizadas ao ambiente de produção, bem como manter a confidencialidade dos dados que constam em ambiente de produção.

3.10. Desenvolvimento Seguro

As recomendações de segurança devem ser analisadas e incluídas em todas as fases do ciclo de vida do desenvolvimento dos sistemas e validadas através de testes de segurança e análise de código.

3.11. Tratamento da Informação

Toda informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação e Privacidade de Dados durante todo o ciclo de vida.

4. DIVULGAÇÃO DO CONTEÚDO

Esta versão deve ser para publicação nos veículos de comunicação externa da Omni, alinhada com a Política Interna de Segurança da Informação e Cibernética.