Política de cibersegurança e proteção de dados

Grupo Syscamp
Área de Atuação: Segurança Eletrônica

1. Introdução

A Syscamp está comprometida em garantir a proteção e a integridade dos dados e sistemas que utiliza em suas operações. Embora não tratemos ou armazenemos dados sensíveis de usuários dos sistemas, nossa política de cibersegurança e segurança da informação visa proteger nossos ativos digitais, a continuidade dos serviços e a confiança dos nossos clientes.

2. Política de Cibersegurança

2.1. Objetivo

Proteger os sistemas, redes e dados da empresa contra ameaças cibernéticas, como ataques de hackers, malware, phishing e outras formas de violação digital. Garantir a resiliência da infraestrutura tecnológica, assegurando a continuidade das operações.

2.2. Escopo

Esta política aplica-se a todos os sistemas, redes e dispositivos digitais utilizados pela Syscamp, abrangendo colaboradores, sócios, fornecedores e parceiros que têm acesso aos recursos tecnológicos da empresa.

2.3. Diretrizes de Cibersegurança

2.3.1. Proteção de Infraestrutura

Todas as redes e sistemas críticos da empresa devem estar protegidos por soluções robustas de segurança, como firewalls, sistemas de detecção de intrusões (IDS), e software antivírus atualizado.

2.3.2. Segurança de Dispositivos

Todos os dispositivos utilizados por colaboradores e parceiros, como computadores, tablets e smartphones, devem ser protegidos com senhas fortes, criptografia e medidas de controle de acesso.

2.3.3. Controle de Acesso

O acesso aos sistemas e redes da empresa será concedido apenas a pessoas autorizadas, conforme suas funções. Devem ser implementados mecanismos de autenticação multifator para proteger contas e evitar acessos não autorizados.

2.3.4. Backup e Recuperação de Dados

Os dados e sistemas críticos da empresa devem ser regularmente copiados em backups seguros. Procedimentos de recuperação de desastres devem ser implementados para garantir a restauração rápida dos serviços em caso de incidentes.

2.3.5. Prevenção de Ataques

A empresa adota medidas proativas de proteção contra ameaças cibernéticas, como testes periódicos de vulnerabilidades e simulações de ataques (pentests) para identificar e corrigir possíveis falhas de segurança.

2.4. Responsabilidades

- ***Equipe de TI:*** *Implementar e monitorar as práticas de cibersegurança, bem como realizar auditorias e testes de segurança.*
- ***Colaboradores:*** *Seguir as práticas recomendadas de cibersegurança e reportar imediatamente qualquer atividade suspeita.*
- ***Fornecedores e Parceiros:*** *Garantir que suas práticas e sistemas estejam alinhados com os padrões de segurança da empresa.*

3. Política de Segurança da Informação

3.1. Objetivo

Garantir a confidencialidade, integridade e disponibilidade das informações corporativas, protegendo os ativos de informação contra acessos não autorizados, alterações e destruição.

3.2. Escopo

Aplica-se a todas as informações, digitais ou físicas, processadas ou armazenadas pela empresa, abrangendo documentos operacionais, contratos e dados de clientes e parceiros. Como não tratamos dados sensíveis de usuários dos sistemas, esta política foca na proteção das informações internas e estratégicas da empresa.

3.3. Diretrizes de Segurança da Informação

3.3.1. Classificação da Informação

As informações da empresa devem ser classificadas de acordo com seu nível de sensibilidade: pública, interna, confidencial e altamente confidencial. Medidas de proteção apropriadas devem ser aplicadas com base nessa classificação.

3.3.2. Controle de Acesso à Informação

Somente pessoas autorizadas terão acesso às informações classificadas. O controle de acesso deve ser baseado no princípio de privilégio mínimo, garantindo que cada pessoa tenha acesso apenas ao que for necessário para suas funções.

3.3.3. Proteção de Informações Físicas e Digitais

Informações confidenciais devem ser protegidas tanto em formato físico (ex: documentos impressos) quanto digital. Documentos físicos devem ser armazenados em locais seguros, e informações digitais devem ser criptografadas, quando necessário.

3.3.4. Uso Adequado de Recursos de Informação

Todos os colaboradores e parceiros devem usar os recursos de informação da empresa de maneira ética e em conformidade com as diretrizes estabelecidas. O uso inadequado ou negligente das informações pode resultar em sanções.

3.3.5. Manutenção e Descarte de Informações

Informações sensíveis ou confidenciais devem ser armazenadas de maneira segura e somente pelo tempo necessário para sua finalidade. O descarte de informações deve ser feito de forma que elas não possam ser recuperadas, como destruição física ou digital segura.

3.4. Treinamento e Conscientização

A empresa oferece treinamentos periódicos sobre boas práticas de segurança da informação, conscientizando colaboradores, fornecedores e parceiros sobre os riscos de vazamento de informações e como evitá-los.

4. Gestão de Incidentes de Segurança

4.1. Detecção de Incidentes

A empresa implementa ferramentas e processos para monitorar suas redes e sistemas, com o objetivo de detectar rapidamente qualquer tentativa de violação de segurança ou uso indevido de informações.

4.2. Resposta a Incidentes

Em caso de incidente de segurança, um plano de resposta será imediatamente acionado. Isso inclui:

- *Isolamento do sistema afetado.*
- *Avaliação do impacto e da extensão do incidente.*
- *Comunicação rápida aos responsáveis e, quando necessário, aos clientes e parceiros.*

4.3. Relatório e Aprendizado

Todos os incidentes serão documentados, e uma análise posterior será conduzida para identificar a causa raiz e as medidas corretivas a serem implementadas, evitando que ocorram novamente.

5. Conformidade e Revisão

A empresa compromete-se a revisar periodicamente suas políticas de cibersegurança e segurança da informação, garantindo que elas estejam alinhadas com as melhores práticas de mercado e regulamentações aplicáveis. Auditorias internas serão realizadas para assegurar o cumprimento das políticas, e atualizações serão implementadas conforme necessário.