UNIVERSIDADE SÃO JUDAS TADEU – USTJ
SISTEMAS COMPUTACIONAIS E SERGURANÇA

Arthur Frederico Piasse Pereira - 824219186

Guilherme Pereira da Silva – 825129559

Jhonatan de Lima Alves dos Santos – 824215769

Sophia Grave Silva - 824213875

Zahra Neqcha - 824221748

DESENVOLVIMENTO DE POLÍTICAS DE SEGURANÇA PARA CONTROTEC

São Paulo
2025

Arthur Frederico Piasse Pereira - 824219186

Guilherme Pereira da Silva – 825129559

Jhonatan de Lima Alves dos Santos – 824215769

Sophia Grave Silva - 824213875

Zahra Neqcha - 824221748

DESENVOLVIMENTO DE POLÍTICAS DE SEGURANÇA PARA CONTROTEC

Este documento apresenta um conjunto básico de políticas de segurança da informação desenvolvidas para uma pequena empresa fictícia do comércio eletrônico, denominada "Controtec". O objetivo é fornecer diretrizes claras para proteção de ativos, mitigação de riscos e conformidade com boas práticas e normas vigentes, como a ISO/IEC 27001 e a Lei Geral de Proteção de Dados (LGPD).

Orientador: Prof. Robson Calvetti

São Paulo
2025

SUMÁRIO

1 INTRODUÇÃO 4
2 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO 5
3 CONSIDERAÇÕES FINAIS 7
4 REFERÊNCIAS 8

1 INTRODUÇÃO

A Controtec é uma empresa do setor varejista e atacadista especializada na comercialização de produtos eletrônicos, localizada no centro de São Paulo. Atuando no atendimento e inovação tecnológica, a empresa busca constantemente aprimorar seus processos operacionais e administrativos para garantir a qualidade de seus serviços e a confiança de seus clientes.

Com a tecnologia avançada, a Controtec reconhece a importância da segurança da informação como um fator estratégico, adotando práticas e políticas que assegurem a confidencialidade, integridade e disponibilidade dos dados.

O presente documento apresenta as Políticas de Segurança da Informação da Controtec, estruturadas de forma a estabelecer diretrizes claras quanto ao acesso e controle de usuários, uso de dispositivos e redes, resposta a incidentes e continuidade dos negócios. Tais medidas visam não apenas a proteção da infraestrutura tecnológica da empresa, mas também o cumprimento das exigências legais, como a Lei Geral de Proteção de Dados (LGPD), e o fortalecimento da cultura de segurança entre os colaboradores.

2 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

2.1 POLÍTICA DE ACESSO E CONTROLE DE USUÁRIO

- O controle de acesso será baseado em função (RBAC), garantindo que cada colaborador tenha acesso apenas às informações necessárias para o desempenho de suas funções.
- Todos os usuários devem utilizar senhas fortes, com no mínimo dez caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos. As senhas devem ser trocadas a cada 90 dias.
- A autenticação multifator (MFA) será implementada para sistemas administrativos. Contas de usuários desligados serão desativadas imediatamente. Contas temporárias terão prazo de expiração definido.

Justificativa: Reduzir o risco de acesso não autorizado e garantir a confidencialidade das informações.

2.2 POLÍTICA DE USO DE DISPOSITIVOS MÓVEIS E REDES

- O uso de dispositivos pessoais para acessar sistemas corporativos é proibido. Somente dispositivos fornecidos pela empresa, devidamente configurados, poderão ser utilizados.
- O acesso remoto será permitido apenas por meio de VPN corporativa com autenticação segura.
- É proibido o uso de redes públicas para acessar os sistemas da empresa.
- O uso de dispositivos USB será restrito. Quando necessário, deverão ser autorizados e possuir criptografia.

Justificativa: Proteger os dados da empresa e de seus clientes contra vazamentos, perdas e acessos indevidos.

2.3 DIRETRIZES PARA RESPOSTA A INCIDENTES DE SEGURANÇA

- Qualquer anomalia ou atividade suspeita deverá ser reportada imediatamente à equipe responsável.
- Será instituída uma Equipe de Resposta a Incidentes (ERI), encarregada de conter, investigar e documentar os incidentes.
- Em casos que envolvam dados de clientes, a comunicação será conduzida de forma transparente, respeitando a LGPD.

Justificativa: Garantir resposta rápida e eficaz, minimizando danos e prevenindo recorrência.

2.4 DIRETRIZES PARA RESPOSTA A INCIDENTES DE SEGURANÇA

Backups automáticos dos dados críticos serão realizados diariamente. As cópias serão armazenadas localmente e em nuvem.

- Todos os backups devem ser protegidos por criptografia e armazenados em locais com controle de acesso físico e lógico.
- Testes de restauração serão realizados trimestralmente para garantir a integridade dos dados.
- A empresa manterá um Plano de Continuidade de Negócios (PCN) com orientações claras para retomada das operações após desastres.

  Justificativa: Assegurar a continuidade dos serviços e integridade das informações em caso de falhas ou incidentes críticos.

3 CONSIDERAÇÕES FINAIS

As políticas aqui propostas foram desenvolvidas com base no perfil da Controtec, respeitando suas operações no comércio eletrônico e físico, e considerando os riscos reais que uma empresa no centro de São Paulo enfrenta. A implementação dessas diretrizes é essencial para garantir a proteção das informações e a continuidade dos negócios.

4 REFERÊNCIAS

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2022 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2022.
- BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018.
- SANS INSTITUTE. Security Policy Templates. Disponível em: <https://www.sans.org/information-security-policy/>. Acesso em: [DATA].