UNIVERSIDADE SÃO JUDAS TADEU

SISTEMAS COMPUTACIONAIS E SEGURANÇA

ALUNOS:

BOAZ MOREIRA CIRINO - RA: 825146412

DANIEL SOUZA BEZERRA - RA: 825158378

EMILYN CARDOSO – RA: 824214832

MICAEL WILLIAM - RA: 824213069

SÃO PAULO

2025

Políticas de Segurança da Informação
Empresa Fictícia: Soluções Web Ágil Ltda.

Introdução

Este documento apresenta um conjunto básico de políticas de segurança da informação desenvolvidas para a empresa fictícia Soluções Web Ágil Ltda., uma pequena empresa de tecnologia especializada em desenvolvimento de sites e sistemas web para clientes de pequeno e médio porte.

As políticas aqui descritas têm como objetivo proteger os ativos digitais da empresa, garantir a continuidade dos serviços e reduzir os riscos associados ao uso indevido de informações e sistemas.

Política de Acesso e Controle de Usuários

Diretrizes:
- Cada colaborador deve possuir um login individual e intransferível.
- O acesso aos sistemas e dados deve seguir o princípio do menor privilégio.
- O uso de autenticação multifator (MFA) será obrigatório para sistemas críticos e para acesso remoto.
- Contas inativas por mais de 30 dias devem ser desativadas automaticamente.
- Processos de admissão e desligamento devem incluir criação e revogação de acessos de forma padronizada e rápida.

Justificativa:
Garantir que apenas pessoas autorizadas acessem informações sensíveis evita vazamentos, fraudes e alterações indevidas.

Política de Uso de Dispositivos Móveis e Redes

Diretrizes:
- Dispositivos móveis usados para trabalho devem ter criptografia de dados ativada e senha de bloqueio.
- É proibido o uso de redes Wi-Fi públicas sem o uso de VPN corporativa.
- A empresa disponibilizará VPN para acesso remoto seguro aos servidores internos.
- A instalação de aplicativos deve ser limitada aos autorizados pela empresa.
- Deve ser feito o controle e inventário de todos os dispositivos utilizados para fins corporativos.

Justificativa:
Dispositivos móveis e redes não seguras aumentam o risco de interceptações e perdas de dados.

Diretrizes para Resposta a Incidentes de Segurança

Diretrizes:
- Todos os colaboradores devem ser treinados para identificar e relatar incidentes de segurança.
- Deve existir um plano de resposta a incidentes com papéis definidos.
- Incidentes devem ser registrados, analisados e documentados.
- Após um incidente, deve ser realizada uma análise de causa raiz e medidas preventivas devem ser adotadas.

Justificativa:
Ter um plano de ação reduz o impacto de incidentes, permite respostas rápidas e evita que o problema se repita.

Política de Backup e Recuperação de Desastres

Diretrizes:
- Backups completos devem ser realizados semanalmente e incrementais diariamente.
- Cópias de backup devem ser armazenadas em local seguro e separado do servidor principal.
- Testes de restauração devem ser realizados trimestralmente.
- Deve ser acionado o Plano de Recuperação de Desastres em caso de falhas graves.

Justificativa:
Backups regulares garantem que, mesmo diante de falhas ou ataques, a empresa possa se recuperar com o mínimo de prejuízo.

Conclusão

Estas políticas formam a base de um programa de segurança da informação adequado à realidade de uma pequena empresa. Elas devem ser revistas periodicamente e ajustadas conforme a evolução da empresa e do cenário de ameaças.