SEGURANCA E AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Política de Segurança da Informação da AutoSolução

Alan Pablo Alves da Silva
Érica Silva Rodrigues
Pedro Henrique Ribeiro Martins
Enicarlos Pereira Gonçalves Júnior
Gustavo Vaz Fernandes

Diamantina - MG
2024-09-07

Sumário

1 Quem somos, Missão e Objetivos **3**
1.1 Quem somos . . . 3
1.2 Missão da AutoSolução . . . 3
1.3 Objetivos . . . 3

2 Ambiente, Infraestrutura e Sistemas **4**
2.1 layout e infraestrutura . . . 4
2.2 Ambiente Físico . . . 6
2.3 Sistema Web . . . 6
2.4 Visão da AutoSolução . . . 8
2.5 Objetivos a Longo Prazo . . . 8

3 Valores, Análises e Segurança **10**
3.1 Valores da Empresa: . . . 10
3.2 Identificação dos Principais Ativos e Suas Vulnerabilidades . . . 10
3.3 Análise das Ameaças Internas e Externas . . . 11

4 Avaliação de Riscos e Impactos na Segurança **12**
4.1 Avaliação dos Riscos à Segurança da Informação . . . 12
4.2 Descrição dos Possíveis Impactos de Incidentes de Segurança na Empresa . 12

5 Política de Segurança da Informação - Normas e Diretrizes **14**
5.1 Política de Sistemas da Informação da AutoSolução . . . 14
5.2 Diretrizes Gerais . . . 14
5.3 Normas de Segurança . . . 15

6 Política de Segurança da Informação - Procedimentos e Instruções **16**
6.1 Criação e Gerenciamento de Contas de Usuário . . . 16
6.2 Identificação e Relato de Incidentes . . . 16
6.3 Plano de Resposta a Incidentes . . . 16
6.4 Backup e Recuperação de Dados . . . 18
6.5 Treinamento e Conscientização . . . 19
6.6 Gestão de Fornecedores e Terceiros . . . 20
6.7 Revisão Anual da PSI . . . 21
6.8 Responsabilidades . . . 22
6.9 Penalidades por Não Conformidade . . . 22

7 Política de Segurança da Informação - Politicas do Sistema **22**
7.1 Introdução . . . 22

7.2 Política de Gestão de Dados Sensíveis 22
7.3 Gestão de Senhas 23
7.3.1 Utilização dos computadores 23
7.4 Criptografia de Dados e Proteção do Banco de Dados 23
7.5 Monitoramento e Auditoria 24
7.6 Consequências do Não Cumprimento 24

1 Quem somos, Missão e Objetivos

1.1 Quem somos

A AutoSolução é uma empresa de pequeno porte dedicada a serviços de mecânica automotiva. Nossa equipe é composta por 15 colaboradores qualificados, empenhados em fornecer soluções completas e confiáveis para a manutenção e reparo de veículos. Comprometemo-nos com a satisfação e segurança dos nossos clientes em cada atendimento.

1.2 Missão da AutoSolução

Nossa missão é oferecer serviços automotivos de alta qualidade que garantam segurança, eficiência e confiança. Com o objetivo de facilitar a vida das pessoas, a AutoSolução busca entregar soluções rápidas, acessíveis e inovadoras para todas as necessidades de manutenção e reparo de veículos.

1.3 Objetivos

- Excelência no Atendimento: Colocamos o cliente no centro de nossas ações, oferecendo um atendimento personalizado, ágil e transparente, construindo uma relação de confiança duradoura.
- Qualidade e Inovação: Investimos em tecnologia de ponta e em técnicas modernas para assegurar a mais alta qualidade em nossos serviços, mantendo um padrão de desempenho e segurança que nos diferencia no mercado.
- Sustentabilidade e Responsabilidade: Priorizamos práticas sustentáveis e eco-friendly, minimizando o impacto ambiental dos nossos processos e promovendo o uso responsável dos recursos.
- Crescimento Contínuo: Valorizamos o desenvolvimento constante da nossa equipe e a modernização de nossa infraestrutura, o que nos permite expandir de forma sustentável e consolidar nossa posição no mercado automotivo.
- Contribuição para a Comunidade: Buscamos ser uma presença ativa na comunidade, apoiando iniciativas locais e promovendo a conscientização sobre a importância da manutenção preventiva e segura de veículos.

2 Ambiente, Infraestrutura e Sistemas

2.1 layout e infraestrutura

A seguir, apresentamos a planta fictícia da oficina mecânica/lava-jato, ilustrando o layout funcional do espaço dedicado à manutenção de veículos.

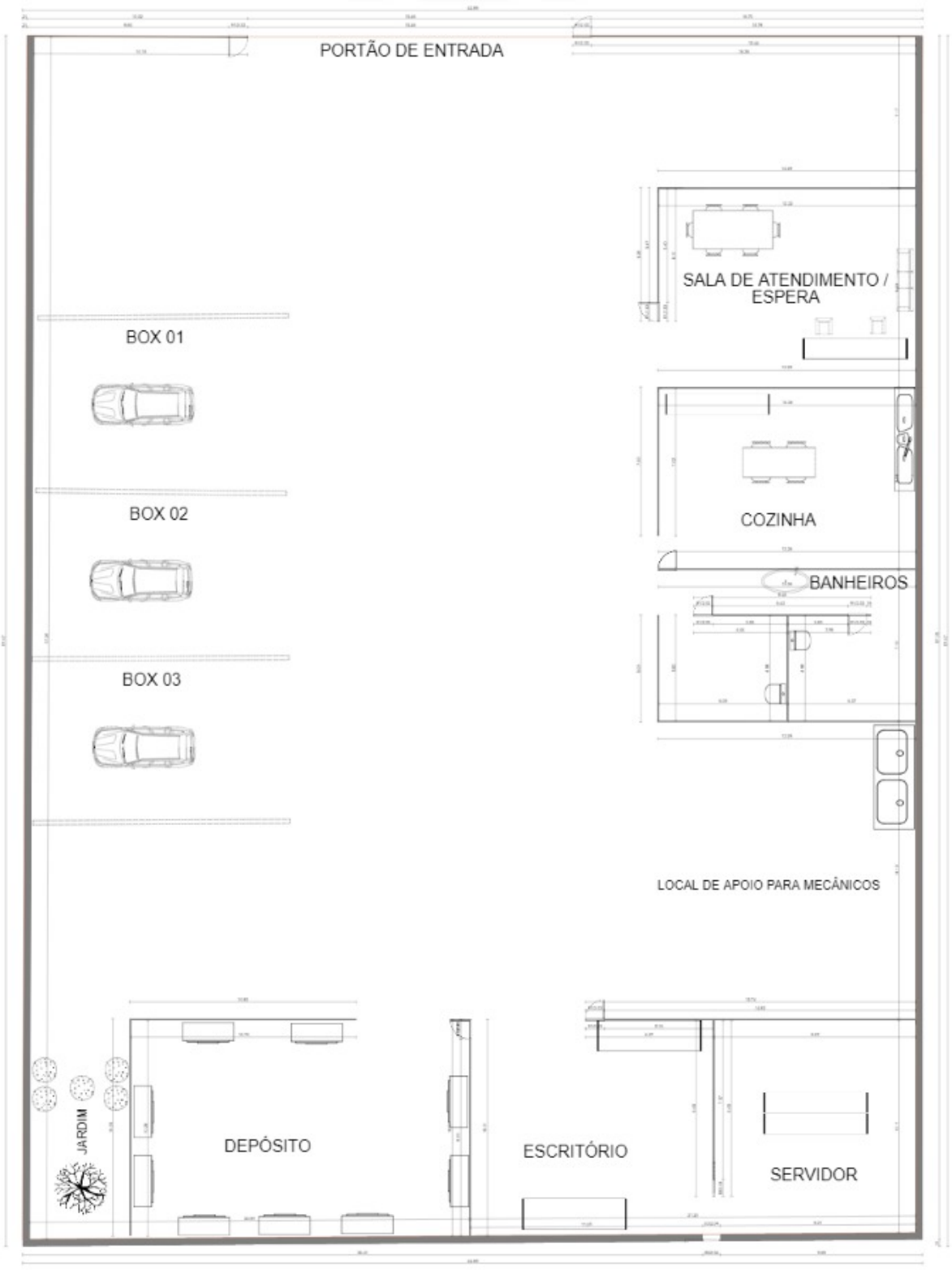

Figura 1: Planta da AutoSolução.

2.2 Ambiente Físico

A AutoSolução possui uma estrutura moderna e bem equipada, projetada para atender eficientemente às necessidades dos nossos clientes. Nosso espaço inclui área para o serviços mecânicos, garantindo uma operação fluida e organizada. O layout é funcional, com zonas bem definidas para atendimento ao cliente, áreas de espera confortáveis, e oficinas separadas para limpeza e manutenção de veículos. A infraestrutura inclui equipamentos de última geração e um sistema de gestão de resíduos para práticas

2.3 Sistema Web

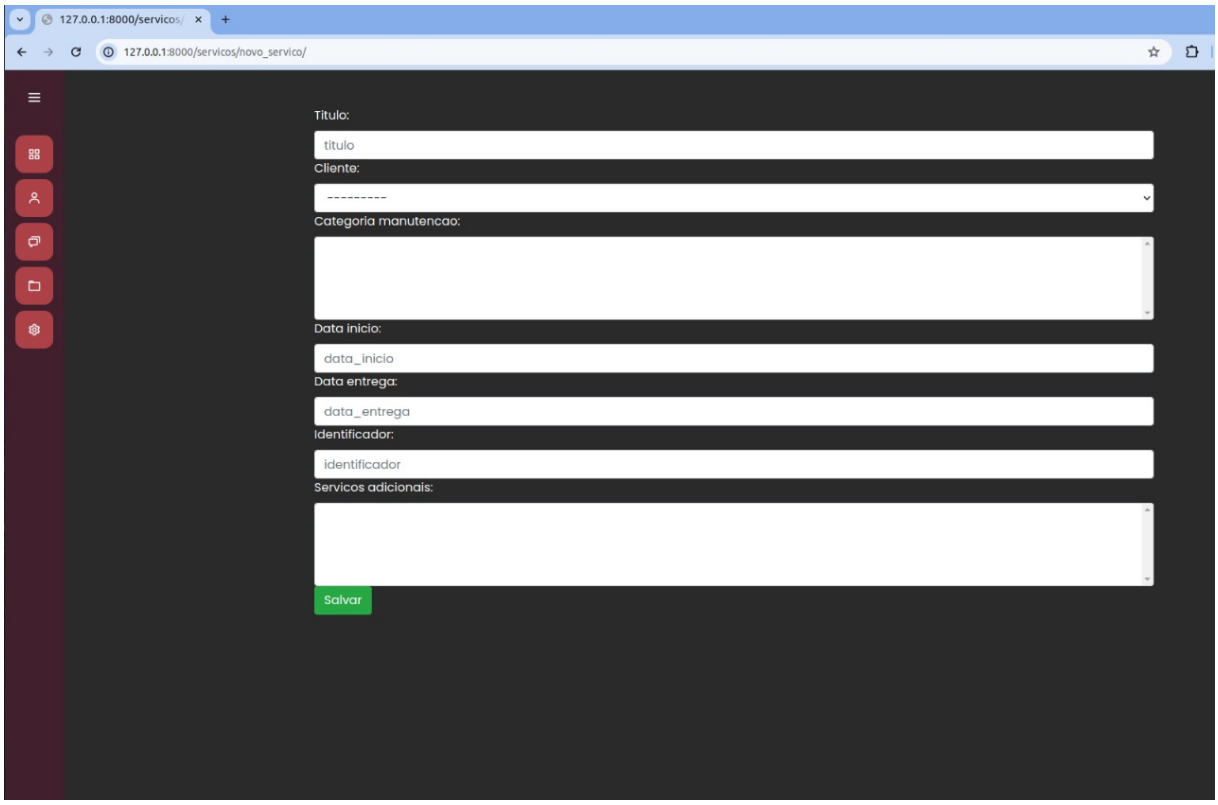

Figura 2: Sistema 1

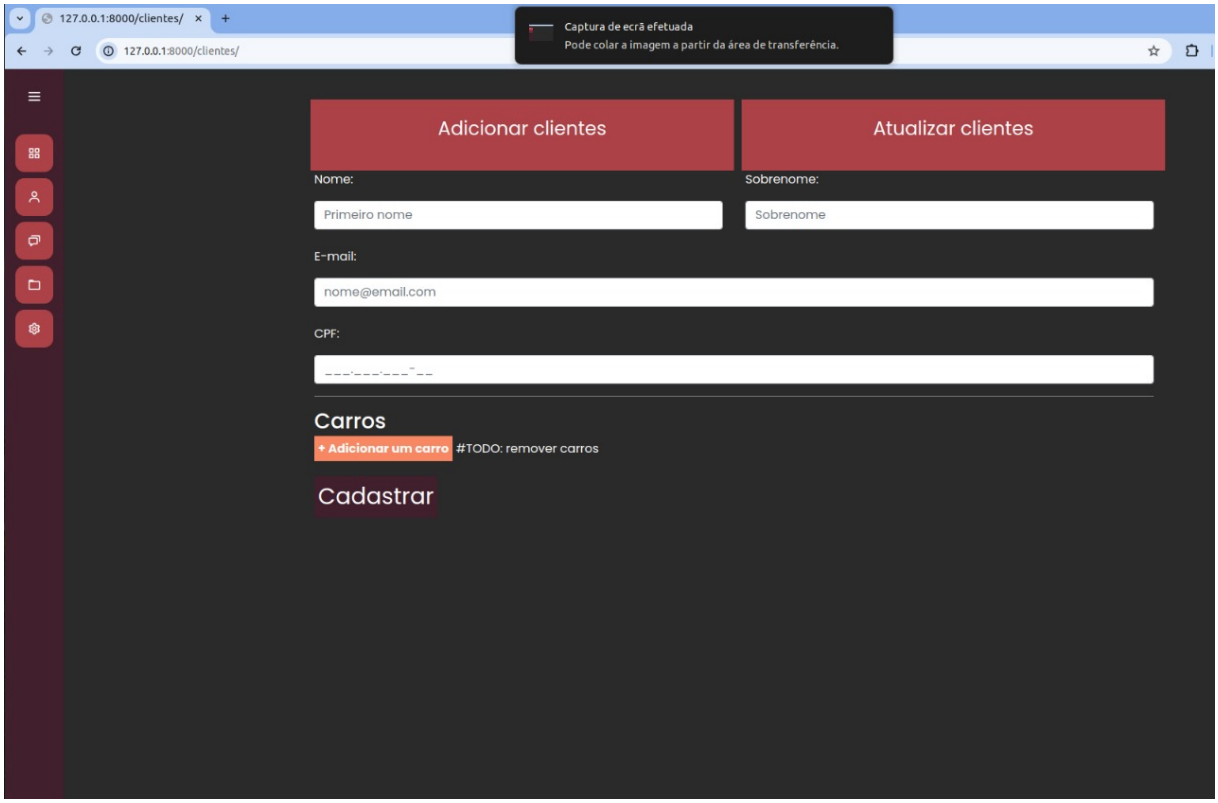

Figura 3: Sistema 2.

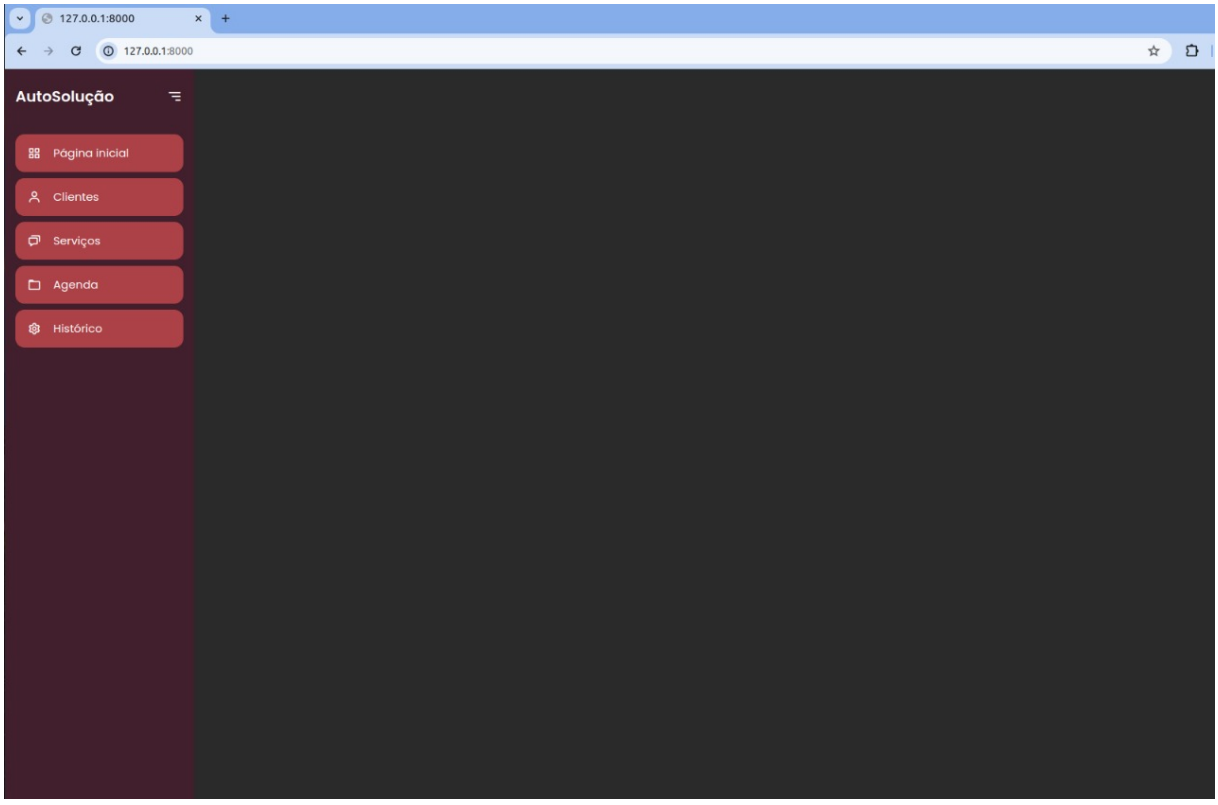

Figura 4: Sistema3

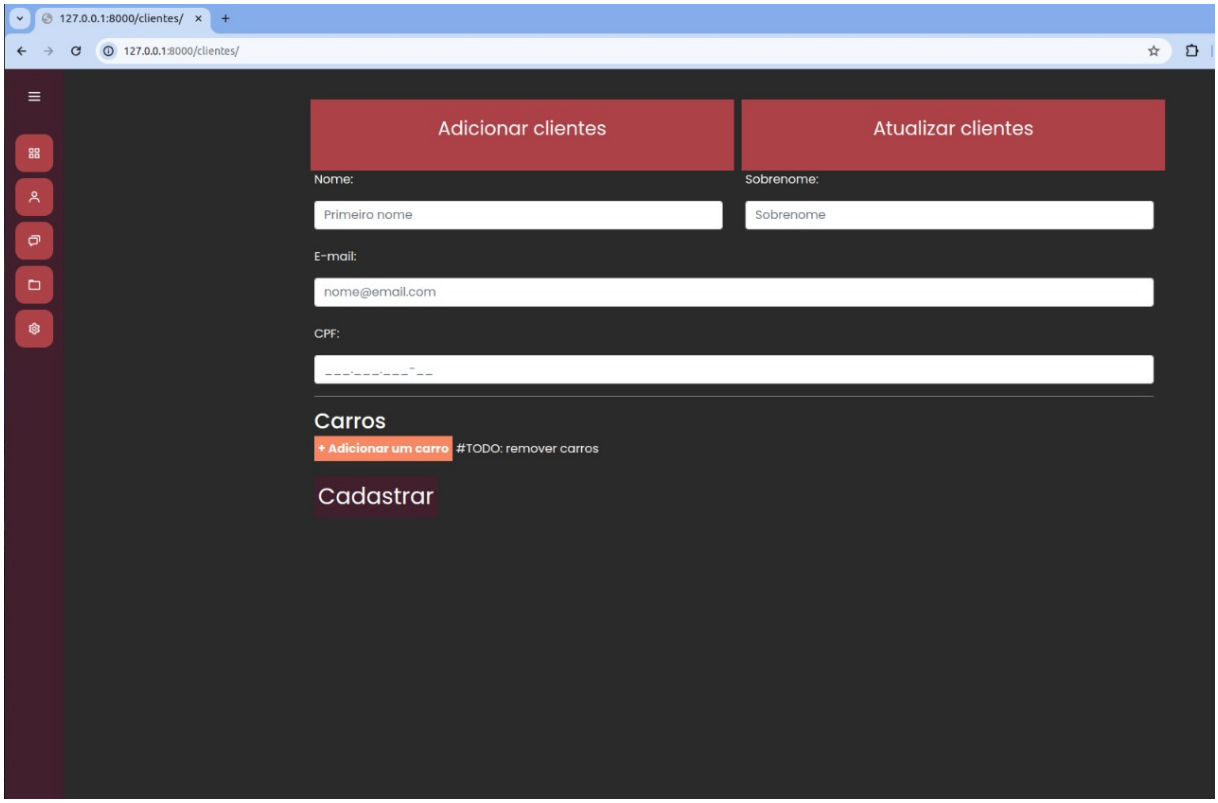

Figura 5: Sistema 4

2.4 Visão da AutoSolução

Ser reconhecida como a principal referência em serviços automotivos na região, destacando-se pela excelência no atendimento, inovação tecnológica e compromisso com a sustentabilidade.

2.5 Objetivos a Longo Prazo

- Liderança Regional: Expandir nossa presença para nos tornarmos a oficina de escolha em toda a região, consolidando nossa marca como sinônimo de confiança e qualidade no setor automotivo.
- Inovação Constante: Investir continuamente em novas tecnologias e práticas de reparo automotivo, promovendo a digitalização dos nossos processos para oferecer soluções mais rápidas e precisas.
- Sustentabilidade e Impacto Social: Alcançar um modelo de negócio totalmente sustentável, com o uso de práticas e materiais eco-friendly, ao mesmo tempo em que contribuímos ativamente para a educação e segurança no trânsito da nossa comunidade.

- Excelência Operacional: Desenvolver uma cultura organizacional focada em melhoria contínua, capacitando nossos colaboradores para alcançar os mais altos padrões de desempenho e serviço.
- Crescimento Sustentável: Expandir nossas operações para outras localidades, sem perder nosso compromisso com a qualidade e a satisfação do cliente, buscando ser uma referência no mercado nacional de serviços automotivos.

3 Valores, Análises e Segurança

3.1 Valores da Empresa:

- Integridade e Transparência: Agir com honestidade e clareza em todas as relações comerciais e internas, mantendo um ambiente de confiança e respeito mútuo.
- Qualidade e Excelência: Buscar a excelência em todos os serviços prestados, garantindo a satisfação do cliente e a segurança de seus veículos.
- Inovação Contínua: Incentivar a inovação e a criatividade, adotando práticas modernas e tecnologias avançadas para melhorar continuamente nossos processos e serviços.
- Sustentabilidade: Comprometimento com práticas sustentáveis, como o uso consciente de água e produtos biodegradáveis, minimizando o impacto ambiental das nossas operações.
- Responsabilidade Social: Contribuir positivamente para a comunidade, promovendo segurança no trânsito e o bem-estar social.
- Valorização do Capital Humano: Investir no desenvolvimento e bem-estar de nossos colaboradores, criando um ambiente de trabalho seguro, inclusivo e motivador.

3.2 Identificação dos Principais Ativos e Suas Vulnerabilidades

- Ativos Físicos: Instalações e Equipamentos: Ferramentas, máquinas de diagnóstico, elevadores automotivos e infraestrutura da oficina. Vulnerabilidades: Desgaste natural, falhas mecânicas, falta de manutenção preventiva e danos acidentais.
- Ativos Humanos: Colaboradores: Equipe de mecânicos, atendentes e gestores. Vulnerabilidades: Riscos ocupacionais, acidentes de trabalho, treinamento inadequado ou falta de conhecimento técnico atualizado.
- Ativos Digitais: Sistemas de Informação: Software de gerenciamento de clientes, dados financeiros e inventário. Vulnerabilidades: Ataques cibernéticos, falhas de software, perda de dados e violações de privacidade.
- Ativos de Reputação: Imagem da Marca: Reputação e confiança conquistada com clientes e parceiros. Vulnerabilidades: Reclamações de clientes, falhas de serviço, práticas comerciais antiéticas.

3.3 Análise das Ameaças Internas e Externas

- Ameaças Internas: Falhas Humanas: Erros operacionais, falta de capacitação adequada, negligência em procedimentos de segurança. Problemas de Infraestrutura: Falta de manutenção preventiva em equipamentos, uso inadequado de ferramentas. Cultura Organizacional: Falta de comunicação eficaz, ambiente de trabalho inseguro, ausência de políticas claras de ética e conformidade.

- Ameaças Externas: Concorrência: Novos entrantes no mercado, concorrentes com ofertas agressivas e inovação constante. Ciberataques: Tentativas de acesso não autorizado a sistemas de informação, roubo de dados e informações sensíveis. Riscos Econômicos e Regulatórios: Instabilidade econômica, mudanças na legislação ambiental ou de segurança do trabalho. Eventos Naturais: Desastres naturais, como inundações ou incêndios, que possam afetar as instalações.

4 Avaliação de Riscos e Impactos na Segurança

4.1 Avaliação dos Riscos à Segurança da Informação

- Ameaças Cibernéticas: Probabilidade: Alta - Devido ao uso de sistemas de gerenciamento digital, há uma alta probabilidade de ataques cibernéticos, como malware, ransomware, e phishing. Impacto: Alto - Acesso não autorizado a dados de clientes e informações financeiras pode resultar em perda financeira, danos à reputação, e potenciais responsabilidades legais.

- Falhas de Sistema e Perda de Dados: Probabilidade: Média - Falhas técnicas, como panes no software de gestão ou servidores fora do ar, podem ocorrer devido à falta de manutenção ou atualização. Impacto: Alto - A perda de dados críticos pode paralisar operações, prejudicar o atendimento ao cliente e gerar custos elevados para recuperação de informações

- Acesso Não Autorizado por Funcionários: Probabilidade: Média - Sem políticas de acesso restritivo e treinamento adequado, funcionários podem acidentalmente ou intencionalmente acessar informações sensíveis. Impacto: Moderado a Alto - Acesso inadequado pode resultar em vazamento de dados ou comprometimento de informações estratégicas.

- Roubo ou Perda de Dispositivos: Probabilidade: Média - Dispositivos móveis como laptops ou tablets usados para operações da empresa podem ser perdidos ou roubados. Impacto: Moderado - Dependendo da sensibilidade dos dados armazenados, pode resultar em vazamento de informações e perda de dados confidenciais.

- Fraude Interna: Probabilidade: Baixa - Embora menos provável, existe o risco de fraude por parte de colaboradores, como manipulação de dados financeiros ou desvio de recursos. Impacto: Alto - Pode levar a perdas financeiras significativas, danos à reputação e questões legais.

- Desastres Naturais: Probabilidade: Baixa - Eventos como incêndios, enchentes ou outras calamidades naturais. Impacto: Alto - Desastres naturais podem danificar instalações, equipamentos e sistemas, resultando em interrupções operacionais significativas.

4.2 Descrição dos Possíveis Impactos de Incidentes de Segurança na Empresa

- Perda Financeira: Incidentes de segurança, como ataques cibernéticos ou fraudes, podem resultar em perdas financeiras diretas devido a roubo de dinheiro ou dados

financeiros, bem como em custos indiretos relacionados à recuperação de sistemas e reparo de danos.

- Danos à Reputação: Vazamentos de dados ou falhas de segurança podem prejudicar a confiança dos clientes e parceiros, levando a perda de negócios, danos à imagem pública, e impactos negativos de longo prazo na reputação da AutoSolução.

- Interrupção das Operações: Falhas de sistemas ou incidentes cibernéticos podem paralisar operações, afetando a capacidade de atender clientes, executar reparos, e manter o fluxo de trabalho, o que pode resultar em perdas de receita e insatisfação do cliente.

- Multas e Penalidades Legais: Incidentes envolvendo o uso inadequado ou vazamento de dados pessoais de clientes podem resultar em penalidades significativas sob leis de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados).

- Perda de Propriedade Intelectual e Dados Confidenciais: O comprometimento de dados internos críticos, como estratégias de negócios, dados financeiros e registros de clientes, pode enfraquecer a posição competitiva da AutoSolução no mercado e expor segredos comerciais.

- Danos ao Relacionamento com Clientes e Parceiros: Incidentes de segurança podem minar a confiança dos clientes e parceiros, levando a cancelamentos de contratos, diminuição da base de clientes, e dificuldades em estabelecer novas parcerias.

- Medidas de Gestão de Riscos: A AutoSolução adota medidas de segurança da informação robustas, como políticas de acesso restritivo, criptografia de dados, treinamento contínuo de funcionários, planos de resposta a incidentes, e backups regulares para mitigar riscos e minimizar o impacto de possíveis incidentes de segurança.

5 Política de Segurança da Informação - Normas e Diretrizes

5.1 Política de Sistemas da Informação da AutoSolução

- Objetivo: Estabelecer diretrizes, normas e procedimentos para proteger os ativos de informação da AutoSolução, garantir a confidencialidade, integridade e disponibilidade das informações, prevenir incidentes de segurança e assegurar o uso ético e responsável dos recursos tecnológicos por todos os colaboradores. Esta política se aplica a todos os colaboradores, prestadores de serviços, parceiros e terceiros que utilizam ou têm acesso aos recursos de TI da AutoSolução.

- Ambito: Esta política abrange todos os sistemas de informação, dispositivos, redes, serviços de armazenamento, aplicações, dados e infraestrutura de TI da AutoSolução, bem como os colaboradores, terceirizados e parceiros que fazem uso destes recursos.

5.2 Diretrizes Gerais

- Segurança da Informação: Assegurar que todas as informações sejam protegidas contra acesso, uso, divulgação, alteração, destruição ou perda não autorizadas. Implementar controles de segurança adequados, incluindo autenticação multifator, criptografia, firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS), e antivírus.

- Confidencialidade dos Dados: Restringir o acesso a informações sensíveis exclusivamente a colaboradores autorizados, de acordo com o princípio do menor privilégio (least privilege). Garantir que todos os dados pessoais e informações confidenciais sejam manipulados conforme as leis aplicáveis, incluindo a LGPD (Lei Geral de Proteção de Dados).

- Integridade e Disponibilidade dos Sistemas: Implementar processos para garantir a precisão e a integridade dos dados e prevenir modificações não autorizadas. Assegurar a disponibilidade contínua dos sistemas e serviços críticos, adotando planos de continuidade de negócios e recuperação de desastres.

- Uso Ético e Responsável dos Recursos Tecnológicos: Os recursos de TI devem ser utilizados exclusivamente para fins relacionados ao trabalho e em conformidade com as políticas internas, leis e regulamentos aplicáveis. Proibir o uso de sistemas e recursos para atividades ilegais, que violem os direitos de terceiros, ou que possam prejudicar a reputação da AutoSolução.

- Conformidade com Leis e Regulamentos: Cumprir todas as leis, regulamentações e normas aplicáveis de proteção de dados, segurança da informação e propriedade intelectual.

- Auditoria e Monitoramento: Realizar auditorias periódicas para verificar a conformidade com esta política. Monitorar continuamente os sistemas de informação para detectar e responder rapidamente a incidentes de segurança.

5.3 Normas de Segurança

- Controle de Acesso: O acesso aos sistemas de informação deve ser concedido com base na necessidade de conhecer (need-to-know) e ser revisado periodicamente. Implementar autenticação multifator (MFA) para todos os sistemas críticos. Proibir o compartilhamento de contas e senhas entre colaboradores.

- Gestão de Senhas: As senhas devem ter, no mínimo, 12 caracteres e incluir uma combinação de letras maiúsculas, minúsculas, números e caracteres especiais. As senhas devem ser trocadas a cada 90 dias e não podem ser repetidas por pelo menos 5 ciclos de troca. É obrigatório o uso de senhas diferentes para sistemas distintos e a utilização de um gerenciador de senhas autorizado pela empresa.

- Proteção de Dados e Backup: Realizar backups diários de todos os dados críticos, armazenando-os em locais seguros e fora das instalações principais. Utilizar criptografia para proteger todos os dados sensíveis durante o armazenamento e transmissão. Realizar testes de recuperação de dados a cada trimestre para verificar a eficácia dos procedimentos de backup.

- Gestão de Incidentes de Segurança: Todo incidente de segurança deve ser imediatamente reportado ao Departamento de Segurança da Informação. Implementar um plano de resposta a incidentes, incluindo identificação, contenção, erradicação, recuperação e análise pós-incidente. Manter um registro detalhado de todos os incidentes de segurança, incluindo medidas tomadas e resultados alcançados.

- Atualizações e Patches de Segurança: Realizar atualizações e aplicar patches de segurança para todos os sistemas operacionais, softwares e aplicativos utilizados na empresa. Monitorar regularmente a conformidade de todos os sistemas com as políticas de atualização e realizar auditorias de segurança.

- Proteção Contra Malwares: Instalar e manter atualizados sistemas antivírus e antimalware em todos os dispositivos da empresa. Configurar políticas de detecção e resposta automática para bloquear e isolar dispositivos suspeitos.

- Uso de Dispositivos Pessoais: Todos os dispositivos pessoais utilizados para acessar os sistemas da AutoSolução devem estar em conformidade com as normas de segurança da empresa, incluindo a instalação de software de gerenciamento de dispositivos móveis (MDM). É proibido o armazenamento de dados confidenciais em dispositivos pessoais sem criptografia e autorização explícita.
- Segurança Física: Implementar controles de acesso físico às instalações da empresa, incluindo áreas restritas de TI e locais de armazenamento de dados. Utilizar câmeras de segurança, crachás de identificação e sistemas de controle de acesso para monitorar a entrada e saída de pessoas.

6 Política de Segurança da Informação - Procedimentos e Instruções

6.1 Criação e Gerenciamento de Contas de Usuário

1. O departamento de TI deve criar contas de usuário após a solicitação formal do gestor responsável. As contas de usuário devem ser desativadas imediatamente após a saída do colaborador da empresa. Revisar regularmente os acessos concedidos para garantir conformidade com as necessidades de função.

6.2 Identificação e Relato de Incidentes

1. Todos os colaboradores devem estar atentos a atividades suspeitas e incidentes de segurança, como acessos não autorizados, falhas de sistema ou presença de malware.
   (a) Relato Imediato: Qualquer incidente de segurança detectado deve ser reportado imediatamente ao setor de Segurança da Informação (SI) através do canal designado, garantindo uma resposta rápida.
   (b) Registro do Incidente: O setor de SI manterá um registro detalhado de todos os incidentes reportados, incluindo data, hora, descrição do incidente e as etapas de mitigação aplicadas.

6.3 Plano de Resposta a Incidentes

1. Um plano estruturado de resposta será seguido para mitigar e recuperar de incidentes de segurança de forma eficaz, contendo as seguintes etapas:
   (a) Identificação e Classificação do Incidente:
      i. Avaliar e classificar o incidente com base na gravidade e no potencial impacto nas operações e na integridade dos dados.

ii. Priorizar o incidente, considerando fatores como a sensibilidade dos dados comprometidos e o risco de propagação.

iii. Registro do Incidente: O setor de SI manterá um registro detalhado de todos os incidentes reportados, incluindo data, hora, descrição do incidente e as etapas de mitigação aplicadas.

(b) Contenção do Incidente:

i. Contenção Imediata: Executar ações para conter o incidente no momento, limitando seu alcance e impacto (exemplo: isolamento de sistemas afetados).

ii. Contenção de Curto e Longo Prazo: Implementar medidas temporárias para estabilizar a situação e, em seguida, medidas de longo prazo para garantir que o problema não se repita.

(c) Erradicação da Causa:

i. Identificar e remover a causa raiz do incidente, como software malicioso ou vulnerabilidades exploradas. Executar uma verificação completa nos sistemas afetados para garantir que estejam livres de ameaças.

(d) Recuperação e Restauração de Sistemas:

i. Restaurar as operações normais após a contenção e erradicação do incidente, assegurando que os sistemas e dados estejam totalmente recuperados.

ii. Verificar a integridade dos dados e realizar testes para confirmar que o ambiente está seguro antes de permitir o retorno ao uso normal.

(e) Análise Pós-Incidente e Lições Aprendidas:

i. Após a recuperação, realizar uma análise detalhada do incidente, documentando as causas, as respostas adotadas e a eficácia das ações de mitigação.

ii. Desenvolver um relatório de lições aprendidas e, quando necessário, atualizar políticas e procedimentos de segurança para evitar a recorrência do incidente

(f) Comunicação e Notificação de Incidentes

i. Notificação aos Stakeholders: Se necessário, comunicar o incidente aos stakeholders relevantes, como gestores, parceiros e clientes, especialmente em casos de vazamento de dados ou interrupções significativas nos serviços.

ii. Conformidade com Regulamentações: Em casos de incidentes envolvendo dados pessoais, seguir as diretrizes da LGPD e notificar as autoridades competentes dentro do prazo estabelecido por lei.

(g) Revisão e Melhoria Contínua

i. Revisão de Protocolos de Resposta: Com base nas lições aprendidas, o setor de SI deve revisar e atualizar periodicamente o plano de resposta a incidentes, ajustando protocolos e treinamentos conforme necessário.

ii. Treinamento e Simulações de Incidentes: Realizar treinamentos regulares e simulações de resposta a incidentes para garantir que a equipe esteja preparada e familiarizada com os procedimentos adequados.

6.4 Backup e Recuperação de Dados

(a) Política de Backup

i. Backup Diário Completo: Todos os dados críticos do sistema serão submetidos a um backup completo diariamente, assegurando que informações essenciais estejam protegidas contra perdas ou danos.

ii. Backup Incremental: Quando aplicável, backups incrementais (cópias apenas das alterações realizadas desde o último backup completo) serão realizados ao longo do dia para reduzir o tempo de restauração e assegurar que as últimas atualizações estejam sempre salvas.

iii. Armazenamento Seguro: Os backups serão mantidos em local seguro e fisicamente separado do ambiente de produção, como em servidores dedicados de backup ou em uma solução de armazenamento em nuvem segura com criptografia de ponta a ponta.

(b) Procedimentos de Segurança para Backups

i. Criptografia de Dados: Todos os backups, tanto os armazenados localmente quanto em nuvem, serão criptografados para evitar acesso não autorizado, garantindo a proteção dos dados em trânsito e em repouso.

ii. Acesso Restrito: Apenas pessoal autorizado terá acesso aos backups. O acesso será controlado por autenticação multifatorial (MFA) e registro de acessos, prevenindo o uso indevido dos dados de backup.

(c) Retenção e Rotatividade de Backups

i. Retenção de Backups: Os backups serão retidos por um período de tempo adequado às necessidades da organização, conforme políticas internas e regulamentações aplicáveis. Um esquema de retenção será implementado, mantendo cópias de backup diárias, semanais e mensais conforme necessário.

ii. Rotatividade de Backup: Os backups antigos serão substituídos regularmente de acordo com o cronograma de retenção, assegurando que os dados armazenados estejam atualizados e relevantes, enquanto minimiza o uso de armazenamento.

(d) Testes e Verificações de Recuperação

i. Testes Regulares de Recuperação: Procedimentos de recuperação serão testados trimestralmente para verificar a integridade dos dados e garantir que os backups possam ser restaurados rapidamente em caso de perda de dados ou falha de sistema.

ii. Documentação dos Testes: Cada teste de recuperação será documentado, incluindo resultados e tempo de restauração, para monitorar a eficácia e ajustar os processos conforme necessário.

(e) Procedimentos de Recuperação de Dados

i. Plano de Recuperação: Em caso de incidente, o setor de TI seguirá um plano de recuperação documentado para restaurar os dados de backup de forma segura e eficiente.

ii. Prioridade na Recuperação: A recuperação priorizará dados e sistemas críticos para minimizar o impacto nas operações da empresa e assegurar que o ambiente esteja totalmente operacional o mais rápido possível.

iii. Confirmação da Integridade dos Dados: Após a restauração, uma verificação de integridade será realizada para garantir que todos os dados foram recuperados corretamente e estão prontos para uso.

(f) Revisão e Melhoria dos Processos de Backup e Recuperação

i. Avaliação Periódica: O processo de backup e recuperação será revisado regularmente para acompanhar mudanças tecnológicas e regulatórias, garantindo que esteja alinhado com as melhores práticas.

ii. Atualização de Procedimentos: Com base nas análises, quaisquer ajustes necessários serão aplicados aos processos de backup e recuperação para fortalecer a segurança e confiabilidade do sistema.

6.5 Treinamento e Conscientização

2. Treinamento Inicial em Segurança da Informação

(a) Sessões de Treinamento Inicial: Todos os colaboradores passarão por um treinamento inicial sobre segurança da informação ao ingressar na organização. Esse treinamento cobrirá as diretrizes básicas de segurança, práticas seguras de uso dos sistemas e a importância da proteção de dados.

(b) Conteúdo Programático: O treinamento inicial incluirá tópicos como

i. Conceitos básicos de segurança da informação (confidencialidade, integridade e disponibilidade).

ii. Identificação e prevenção de ameaças comuns, como phishing, malware e ataques de engenharia social.

iii. Uso seguro de senhas e autenticação multifatorial (MFA).

iv. Políticas internas de manuseio e proteção de dados sensíveis.

(c) Sessões Periódicas de Atualização

i. Frequência de Atualização: Sessões de atualização serão realizadas semestralmente para todos os colaboradores, abordando novas ameaças e atualizações nas políticas e práticas de segurança da organização.

ii. Conteúdos de Atualização: As sessões de atualização cobrirão tópicos recentes e adaptarão as práticas de segurança aos novos cenários, incluindo:

A. Boas práticas para proteção de dispositivos e dados pessoais.

B. Protocolos de resposta a incidentes e reporte de atividades suspeitas.

C. Novas ferramentas e atualizações de segurança implementadas no sistema.

(d) Campanhas de Conscientização

i. Ações de Sensibilização: A organização promoverá campanhas regulares de conscientização sobre segurança da informação, como e-mails informativos, cartazes e notificações nos sistemas, para reforçar práticas seguras no dia a dia dos colaboradores.

ii. Exercícios de Simulação: Simulações práticas, como testes de phishing, serão realizadas para avaliar e aprimorar a capacidade dos colaboradores de identificar e responder a ameaças comuns. Feedbacks individuais serão fornecidos para incentivar o aprendizado.

(e) Responsabilidade Individual e Cultura de Segurança

i. Incentivo à Responsabilidade: Todos os colaboradores são incentivados a adotar uma postura proativa e responsável em relação à segurança, reconhecendo seu papel na proteção dos ativos informacionais da organização.

ii. Relato de Incidentes e Ameaças: Os colaboradores serão treinados para reportar imediatamente qualquer comportamento suspeito ou incidente de segurança ao setor de Segurança da Informação, sem medo de represálias.

6.6 Gestão de Fornecedores e Terceiros

1. Avaliar os riscos de segurança associados a fornecedores e terceiros antes de estabelecer qualquer contrato. Exigir que todos os fornecedores e terceiros cumpram as políticas de segurança da AutoSolução e assinem um termo de confidencialidade.

6.7 Revisão Anual da PSI

1. **Periodicidade de Revisão:** A Política de Segurança da Informação (PSI) será revisada anualmente para assegurar que se mantenha alinhada com as melhores práticas de segurança e as necessidades operacionais da organização.

2. **Responsáveis pela Revisão:** A revisão será conduzida pelo Comitê de Segurança da Informação, com participação de representantes das áreas de TI, compliance e gestão, para garantir uma análise abrangente e atualizada.

Revisão em Caso de Mudanças Significativas

1. **Mudanças em Requisitos de Segurança:** A PSI será revisada sempre que houver alterações significativas nos requisitos de segurança, como novas regulamentações (ex.: mudanças na LGPD), padrões de conformidade ou práticas de segurança recomendadas.

2. **Alterações no Ambiente de TI:** Caso ocorram mudanças estruturais no ambiente de TI, como a implementação de novas tecnologias, sistemas ou mudanças na infraestrutura de rede, a PSI será atualizada para cobrir novos riscos e requisitos de segurança.

Avaliação de Efetividade e Melhoria Contínua

1. **Monitoramento de Conformidade:** Durante a revisão, será avaliada a conformidade dos colaboradores com as políticas estabelecidas, considerando feedbacks de incidentes e os resultados dos treinamentos realizados ao longo do ano.

2. **Incorporação de Lições Aprendidas:** Todas as lições aprendidas de incidentes de segurança ou simulações serão incorporadas à política para fortalecer a proteção e responder a ameaças emergentes.

Processo de Aprovação e Comunicação

1. **Aprovação da Alta Gestão:** A nova versão da PSI será aprovada pela alta gestão antes de ser implementada, garantindo que a política reflita os objetivos estratégicos da organização em segurança da informação.

2. **Divulgação aos Colaboradores e Partes Interessadas:** Uma vez aprovada, a versão atualizada da PSI será comunicada a todos os colaboradores e partes interessadas. Treinamentos ou sessões informativas serão organizados para garantir a compreensão das novas diretrizes.

Documentação e Controle de Versões

1. **Histórico de Revisões:** Cada versão da PSI será documentada com um registro das alterações realizadas, incluindo a data e os responsáveis pela atualização, para manter um histórico de revisões.

2. **Controle de Acesso:** A política revisada será disponibilizada de maneira segura e acessível aos colaboradores, assegurando que a versão mais recente esteja sempre em vigor e aplicada.

6.8 Responsabilidades

1. Todos os Colaboradores: Cumprir as diretrizes, normas e procedimentos estabelecidos nesta política e reportar imediatamente qualquer incidente ou suspeita de incidente de segurança. Departamento de TI: Implementar, monitorar e atualizar as medidas de segurança, gerenciar incidentes de segurança, e realizar auditorias e manutenções necessárias. Gestores: Garantir que todos os membros da equipe estejam cientes e cumpram esta política, além de fornecer suporte na implementação e manutenção dos controles de segurança.

6.9 Penalidades por Não Conformidade

1. O não cumprimento desta política pode resultar em ações disciplinares, que variam de advertências até demissão, conforme a gravidade da violação e os regulamentos internos da AutoSolução. Essa política de sistemas da informação proporciona um ambiente seguro e resiliente, mitigando riscos e assegurando a continuidade das operações, protegendo tanto os dados da empresa quanto às informações de seus clientes e parceiros.

7 Política de Segurança da Informação - Politicas do Sistema

7.1 Introdução

Para garantir a segurança do sistema AutoSolução, aqui estão algumas diretrizes específicas de políticas de segurança da informação, visando apenas o sistema.

7.2 Política de Gestão de Dados Sensíveis

Armazenamento Seguro: Todos os dados considerados sensíveis devem ser criptografados, tanto em repouso (armazenados) quanto em trânsito (durante a transmissão). Dados

sensíveis não devem ser armazenados fora das plataformas autorizadas pela AutoSolução, como em dispositivos pessoais.

7.3 Gestão de Senhas

A AutoSolução implementará políticas de gestão de senhas, que incluem o uso de senhas fortes, a exigência de mudanças periódicas e a proibição do compartilhamento de senhas entre colaboradores. A autenticação multifatorial (MFA) será aplicada em todos os sistemas críticos da empresa. Além disso, as senhas devem atender aos seguintes requisitos mínimos: - Ter no mínimo 8 caracteres; - Não ser uma senha comum ou facilmente previsível; - Contemplar ao menos uma letra minúscula, uma letra maiúscula, um número e um caractere especial.

7.3.1 Utilização dos computadores

Bloquear o acesso a sites de risco: Utilizar ferramentas de segurança nos computadores da empresa, como firewalls e filtros de conteúdo, para bloquear o acesso a sites conhecidos por serem maliciosos ou que apresentem conteúdo inadequado.

Regras para acesso a internet: O acesso a sites da internet deve ser feito de forma responsável e segura. É proibido o acesso a sites que contenham conteúdo ilegal, ofensivo ou que representem risco à segurança da informação, como sites de jogos, redes sociais e sites de downloads não confiáveis. A empresa utiliza ferramentas de segurança para bloquear o acesso a sites maliciosos e monitorar o tráfego de rede.

Downloads: É proibido baixar, executar ou utilizar arquivos oriundos da internet, mídias removíveis e outros. Além de ser proibido baixar mídias como músicas, filmes, fotos e etc.

Mídias Removíveis: O uso de mídias removíveis, como pen drives, HDs externos e cartões de memória, é proibido nos computadores da empresa, exceto em casos autorizados e com dispositivos previamente escaneados e aprovados pelo departamento de TI.

7.4 Criptografia de Dados e Proteção do Banco de Dados

Criptografia de Dados: Informações sensíveis de clientes (por exemplo, dados pessoais, dados de transações) devem ser criptografadas tanto em repouso quanto em trânsito, utilizando algoritmos robustos de criptografia (como AES-256).

Protocolos Seguros de Comunicação: Toda comunicação entre cliente e servidor deve utilizar o protocolo TLS 1.3 para garantir a proteção contra interceptação de dados.

7.5 Monitoramento e Auditoria

Implementar mecanismos de monitoramento contínuo para detectar atividades suspeitas e incidentes de segurança. Planejar e realizar auditorias de segurança periódicas para avaliar a efetividade das medidas de segurança e identificar possíveis vulnerabilidades.

7.6 Consequências do Não Cumprimento

O não cumprimento das diretrizes de segurança da informação aqui estabelecidas poderá resultar em medidas disciplinares, que podem variar de acordo com a gravidade da infração, incluindo:

Advertência verbal ou escrita: Para infrações leves ou de primeira ocorrência.

Suspensão do acesso aos sistemas: Em casos de violações que comprometam a segurança dos dados.

Multa: Dependendo da natureza da infração e dos danos causados, poderá ser aplicada multa ao colaborador.

Demissão por justa causa: Em casos de violações graves ou reincidentes, que causem prejuízo significativo à empresa.

Processos judiciais: A AutoSolução se reserva o direito de tomar medidas legais cabíveis em caso de violação da política de segurança que resulte em danos à empresa, a seus clientes ou a terceiros.