# Política de Segurança da Informação

## POL.SI.01

*Política do Sistema de Gestão da Arlequim*

**Sumário**

**Introdução** ..... 3
**Arquitetura de Segurança e Integridade** ..... 3
**Sistemas Desenvolvidos e/ou Adquiridos** ..... 4
**Gerenciamento de Mudanças** ..... 4
**Acesso à Internet** ..... 4
**Acesso Remoto** ..... 5
**Acesso Físico** ..... 5
**Antivírus** ..... 5
**Direitos de Acesso e Senhas** ..... 5
**Política de Backup** ..... 6
**Colaborador** ..... 7
**Obrigações dos Colaboradores** ..... 7
**Mesa Limpa** ..... 7
**Tela Limpa** ..... 8
**BYOD (Bring Your Own Device)** ..... 8
**Utilização Profissional dos Recursos de TI** ..... 9
**Regras de Utilização dos Recursos de TI** ..... 9
**Cuidados com as Senhas e Responsabilidade** ..... 10
**Utilização de Softwares** ..... 10
**Proteção contra Vírus de Computador** ..... 10
**Utilização da Internet** ..... 10
**Rede WiFi** ..... 11
**Demais Recursos de TI** ..... 11
**Alimentos, Bebidas e Afins** ..... 11
**Teletrabalho** ..... 12
**Visitantes** ..... 12
**Clientes** ..... 12
**Terceirização de Serviços** ..... 13
**Auditoria** ..... 13
**Auditoria e Monitoramento** ..... 13
**Plano de Resposta a Incidentes de Segurança** ..... 14
**Requisitos Legais e Normativos** ..... 14

## 1. Missão, Objetivos e Finalidade da Política

A Missão da Política de Segurança da Informação é estabelecer diretrizes para proteger informações corporativas de forma efetiva. Os Objetivos incluem proteção de dados, conformidade regulatória, gestão de riscos, conscientização e treinamento, e resposta a incidentes, buscando manter a integridade, confidencialidade e disponibilidade da informação. A Finalidade é criar um sistema adaptativo e contínuo para proteger os ativos de informação, assegurando a segurança como um processo evolutivo e integrado à cultura organizacional.

## 2. Papéis e Responsabilidades do Processo (MATRIZ RACI)

As responsabilidades relativas à execução, aprovação, consulta e informação das atividades descritas nesta política estão definidas na Matriz RACI Corporativa da Arlequim Technologies. Esse documento centraliza as responsabilidades de todos os processos organizacionais e está mantido em local controlado, sendo revisado periodicamente para garantir sua aderência às funções e estruturas da organização.

## 3. Informação Documentada de Origem Interna e Externa Referenciadas

Todas as informações documentadas exigidas por este procedimento ou referenciadas por este, bem como suas respectivas versões controladas, estão registradas na Lista Mestra de Documentos, conforme definido no Procedimento de Gestão da Arlequim Technologies. Documentos de origem externa que sejam aplicáveis ou necessários para o planejamento, implementação e operação do sistema de gestão também são identificados e controlados por meio da Matriz de Documentos de Origem Externa, assegurando a rastreabilidade, integridade e disponibilidade dessas informações conforme requerido pela ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27701:2019.

## 4. Histórico de Revisões e Aprovações

| Revisão | Data | Elaborador | Revisor | Aprovador | Descrição da Revisão |
|---|---|---|---|---|---|
| **00** | 05/12/2023 | Marco Rockenbach e Edson Nunes | Rafael Rabelo e Guilherme Nocera | Tiago Jesuíno | Emissão Inicial do Documento |
| **01** | 20/03/2025 | Marco Rockenbach e Edson Nunes | Gislaine Mereles, Carlise Amaral e Letícia Melo | Tiago Jesuíno e Alessandra Souza | Revisão Geral da Política |
| **02** | 16/02/2025 | Marco Rockenbach e Edson Nunes | Edson Nunes | Ricardo Floresta | Revisão Geral da Política |

## 5. Descrição das Diretrizes

### 5.1 Introdução

1. **Propósito e Escopo:** A Política de Segurança da Informação (PSI) da Arlequim tem como objetivo principal estabelecer um conjunto de diretrizes e práticas para a proteção das informações corporativas. Estas diretrizes aplicam-se a todos os colaboradores, incluindo a alta direção, funcionários, contratados e terceiros que interagem com os sistemas e dados da empresa. A PSI abrange todos os aspectos da segurança da informação, desde o acesso físico e lógico até a gestão de incidentes e continuidade dos negócios.

2. **Importância da Segurança da Informação:** A segurança da informação é vital para a preservação da confidencialidade, integridade e disponibilidade dos dados da empresa. Em um mundo cada vez mais digitalizado e interconectado, a proteção das informações se torna um componente crítico para a manutenção da reputação, conformidade legal e vantagem competitiva da organização.

3. **Compromisso da Gestão:** A alta direção da empresa compromete-se a prover os recursos necessários para implementar, manter e melhorar continuamente o sistema de gestão de segurança da informação. Este compromisso inclui a realização de avaliações periódicas da eficácia da PSI, garantindo que ela permaneça alinhada com os objetivos estratégicos e operacionais da empresa.

4. **Conscientização e Capacitação:** Uma parte fundamental da PSI é a promoção da sua disseminação, conscientização e capacitação em segurança da informação para todos os colaboradores. Treinamentos regulares, comunicações e exercícios práticos são essenciais para garantir que todos compreendam suas responsabilidades e saibam como agir de maneira segura.

5. **Revisão e Atualização**: A PSI é um documento dinâmico, que deve ser revisado e atualizado regularmente para refletir as mudanças no ambiente de negócios, tecnológico e regulatório. As sugestões de melhorias por parte dos colaboradores são bem-vindas e consideradas parte integrante do processo de melhoria contínua.

### 5.2 Arquitetura de Segurança e Integridade

1. **Desenho da Arquitetura:** A arquitetura de segurança da empresa deve ser desenhada para garantir a integridade, confidencialidade e disponibilidade dos dados. Isso inclui a implementação de camadas múltiplas de defesa, segmentação de rede e controles de acesso robustos.

2. **Princípios de Segurança:** A arquitetura deve ser baseada em princípios de segurança reconhecidos, como o menor privilégio e a defesa em profundidade, garantindo que as defesas sejam eficazes contra uma variedade de ameaças.

3. **Avaliação de Riscos:** Uma avaliação de riscos regular deve ser realizada para identificar e mitigar vulnerabilidades potenciais dentro da arquitetura de TI.

4. **Atualizações e Manutenção:** A infraestrutura de TI deve ser mantida e atualizada regularmente para garantir a proteção contra ameaças emergentes e manter a compatibilidade com os padrões de segurança atuais.

5. **Testes de Intrusão:** Testes de penetração regulares devem ser realizados para avaliar a eficácia da arquitetura de segurança e identificar pontos fracos que necessitem de fortalecimento.

## 5.3 Sistemas Desenvolvidos e/ou Adquiridos

1. **Avaliação de Segurança:** Antes da implementação, todos os sistemas desenvolvidos internamente ou adquiridos devem passar por uma rigorosa avaliação de segurança, incluindo testes de intrusão e avaliação de vulnerabilidades.

2. **Conformidade com Padrões:** Os sistemas devem estar em conformidade com os padrões internacionais de segurança da informação, como ISO/IEC 27001, e devem ser continuamente atualizados para atender a esses padrões.

3. **Gestão de Mudanças:** Qualquer alteração nos sistemas, seja por desenvolvimento interno ou por atualizações de fornecedores, deve seguir um processo estruturado de gestão de mudanças para garantir que a segurança não seja comprometida.

4. **Treinamento e Documentação:** Os colaboradores envolvidos na operação e manutenção dos sistemas devem receber treinamento adequado. Deve haver documentação abrangente disponível para apoiar a operação e a solução de problemas.

5. **Monitoramento e Manutenção Contínuos:** Os sistemas devem ser monitorados constantemente para detectar atividades anormais ou suspeitas. A manutenção regular é essencial para garantir que os sistemas estejam funcionando de forma eficaz e segura.

## 5.4 Gerenciamento de Mudanças

1. **Processo Formalizado:** Um processo formal de gerenciamento de mudanças está estabelecido para controlar todas as alterações nos sistemas de TI, garantindo que as mudanças sejam implementadas de forma segura e eficaz.

2. **Avaliação de Impacto:** Antes de implementar qualquer mudança, deve-se realizar uma avaliação de impacto para entender as implicações na segurança e operação dos sistemas.

3. **Testes e Validação:** As mudanças devem ser testadas em um ambiente controlado antes de serem implementadas na produção, garantindo que não introduzam novas vulnerabilidades.

4. **Comunicação e Documentação:** As mudanças devem ser comunicadas a todas as partes interessadas e devidamente documentadas, incluindo a razão da mudança, os procedimentos realizados e qualquer impacto identificado.

5. **Revisão Pós-Implementação:** Após a implementação, as mudanças devem ser revisadas para garantir que foram bem-sucedidas e não causaram problemas de segurança não intencionais.

## 5.5 Acesso à Internet

1. **Controles de Acesso:** O acesso à Internet deve ser controlado por meio de firewalls, filtros de conteúdo e outras tecnologias de segurança para prevenir o acesso a sites maliciosos ou inapropriados.

2. **Políticas de Uso Aceitável:** Deve haver uma política clara de uso aceitável da Internet, especificando o que é permitido e proibido no uso da Internet no ambiente de trabalho.

3. **Monitoramento do Tráfego:** O tráfego da Internet deve ser monitorado para detectar e bloquear atividades suspeitas, como tentativas de phishing, downloads de malware ou acessos a sites comprometidos.

4. **Educação dos Usuários:** Os colaboradores devem ser educados sobre os riscos associados ao uso da Internet e as melhores práticas para navegar de forma segura.

5. **Segurança em Nível de Rede:** Devem ser implementadas medidas de segurança robustas em nível de rede, incluindo a segregação de redes internas e externas e o uso de VPNs para conexões seguras.

## 5.6 Acesso Remoto

1. **Autenticação Forte:** O acesso remoto aos sistemas da empresa deve ser protegido por autenticação forte, preferencialmente utilizando autenticação com multifator.

2. **Monitoramento e Auditoria:** O acesso remoto pode ser monitorado e auditado para detectar atividades suspeitas ou não autorizadas.

3. **Atualização e Manutenção de Segurança:** As soluções de acesso remoto devem ser mantidas atualizadas com as últimas atualizações de segurança e patches para proteger contra vulnerabilidades conhecidas.

## 5.7 Acesso Físico

1. **Controle de Acesso Físico:** O acesso físico aos recursos críticos de TI, como servidores e centros de dados, deve ser estritamente controlado e monitorado.

2. **Autenticação e Registro:** Deve haver um sistema de autenticação para controlar o acesso às áreas seguras, com registros detalhados e precisos de quem acessou e quando (hora e data).

3. **Medidas de Segurança Física:** Medidas de segurança física, como câmeras de segurança, alarmes e barreiras físicas, devem ser implementadas para proteger os recursos de TI.

4. **Acesso de Visitantes:** O acesso de visitantes às áreas seguras deve ser limitado e monitorado, com acompanhamento de um colaborador autorizado.

## 5.8 Antivírus

1. **Implementação de Antivírus:** Todos os dispositivos que acessam a rede da empresa devem ter uma solução de antivírus instalada e ativa, fornecendo proteção contra malwares e outras ameaças.

2. **Atualizações Constantes**: O software antivírus deve ser configurado para atualizar suas definições de vírus automaticamente, garantindo proteção contra as mais recentes ameaças.

3. **Varreduras e Inspeções Regulares:** Devem ser realizadas varreduras regulares para detectar e remover malwares de dispositivos e redes.

## 5.9 Direitos de Acesso e Senhas

1. **Gerenciamento de Acesso:** Os direitos de acesso aos sistemas e dados da empresa são concedidos com base na função e nas necessidades de cada colaborador. O acesso é restrito ao mínimo necessário para que cada indivíduo possa desempenhar suas funções.

2. **Controle de Senhas:** As senhas são a primeira linha de defesa na proteção de contas e sistemas. Elas devem ser complexas, únicas e mantidas em sigilo. É proibido o compartilhamento de login e senhas entre colaboradores.

3. **Alteração e Recuperação de Senhas:** As senhas devem ser alteradas regularmente e imediatamente se houver suspeita de comprometimento. A empresa deve fornecer um processo seguro para a recuperação ou redefinição de senhas esquecidas.

4. **Uso de Autenticação Multifator:** A autenticação multifator deve ser utilizada para aumentar a segurança do acesso aos sistemas e dados críticos.

5. **Auditoria e Revisão de Acessos:** Os direitos de acesso serão revisados periodicamente para garantir que permaneçam apropriados. Mudanças de função de colaboradores resultarão na revisão de acessos e, em caso de término do contrato de trabalho, resultará em sua revogação.

## 5.10 Política de Backup

1. **Ambientes Sujeitos ao Backup**.

   1.1. **Identificação de Dados Críticos:** O primeiro passo na política de backup é identificar quais dados são críticos para a operação da empresa, o que inclui, mas não se limita a informações financeiras, listagem de fornecedores, dados sensíveis, dados de clientes, documentação de projetos, e-mails corporativos e bases de dados de sistemas internos.

   1.2. **Abrangência dos Ambientes:** O backup deve abranger todos os ambientes onde os dados críticos são armazenados, incluindo servidores, sistemas na nuvem, estações de trabalho e dispositivos móveis.

   1.3. **Classificação e Priorização:** Os dados devem ser classificados e priorizados com base em sua importância e criticidade. Isso ajudará a determinar a frequência e o método de backup mais adequados para cada tipo de dado.

   1.4. **Compliance e Regulamentações:** A política de backup deve estar em conformidade com as regulamentações e leis aplicáveis sobre a retenção e proteção de dados, como a LGPD.

   1.5. **Avaliação e Revisão Contínua:** A lista de ambientes e dados sujeitos a backup deve ser revisada e atualizada regularmente para garantir que todas as informações importantes estejam protegidas.

2. **Rotinas de Backup**

   2.1. **Frequência de Backup:** A frequência dos backups deve ser determinada com base na criticidade dos dados e na velocidade com que eles mudam. Dados mais críticos podem exigir backups diários ou até em tempo real.

   2.2. **Métodos e Tecnologias de Backup:** Devem ser utilizadas tecnologias de backup confiáveis e comprovadas. Isso pode incluir backups em fita, discos ou soluções baseadas em nuvem.

   2.3. **Automação dos Processos:** Sempre que possível, os processos de backup devem ser automatizados para reduzir o risco de erro humano e garantir a consistência na execução dos backups.

   2.4. **Segurança e Criptografia:** Os backups devem ser protegidos com criptografia e armazenados em locais seguros, físicos ou na nuvem, para proteger contra acesso não autorizado e perda de dados.

**2.5. Monitoramento e Logs:** Deve haver um sistema para monitorar o sucesso ou falha dos processos de backup, com logs detalhados que permitam a análise e correção de problemas.

**3. Rotina de Restauração**

**3.1. Procedimentos de Restauração:** Deve haver procedimentos claros e testados para a restauração de dados a partir dos backups, garantindo que os dados possam ser recuperados rapidamente em caso de perda ou corrupção.

**3.2. Testes Periódicos de Restauração:** É crucial realizar testes periódicos de restauração para garantir que os backups estejam funcionando corretamente e que os dados possam ser efetivamente recuperados.

**3.3. Documentação e Treinamento**: Os procedimentos de restauração devem ser bem documentados e a equipe de TI deve ser treinada para executar restaurações de forma eficiente e segura.

**3.4. Avaliação de Impacto da Restauração:** Ao restaurar dados, deve-se avaliar o impacto da restauração nos sistemas atuais e nas operações de negócios, minimizando a interrupção das atividades.

**3.5. Atualização dos Planos de Restauração:** Os planos de restauração devem ser revisados e atualizados regularmente para refletir mudanças no ambiente de TI e nos requisitos de negócios.

## 5.11 Colaborador

1. **Responsabilidade do Colaborador:** Cada colaborador é responsável pela segurança das informações que acessa, processa e armazena. Esta responsabilidade inclui o conhecimento e a adesão a todas as políticas e procedimentos estabelecidos pela empresa e o reporte imediato de qualquer incidente de segurança para o departamento de segurança da informação.

## 5.12 Obrigações dos Colaboradores

1. **Adesão às Políticas:** Todos os colaboradores são obrigados a conhecer e a aderir estritamente às políticas e procedimentos de segurança da informação estabelecidos pela empresa. Isso inclui o cumprimento de todas as diretrizes relacionadas ao uso de recursos de TI, gestão de dados e comunicação.

2. **Responsabilidade por Acessos e Senhas:** Os colaboradores são individualmente responsáveis pela segurança de suas credenciais de acesso e devem garantir que suas senhas sejam fortes, únicas e mantidas em segredo.

3. **Proteção de Informações Confidenciais:** É fundamental que os colaboradores protejam as informações confidenciais da empresa, tanto em formato digital quanto físico, evitando a exposição ou compartilhamento não autorizado.

4. **Reporte de Incidentes:** Os colaboradores devem reportar imediatamente qualquer incidente de segurança da informação ao departamento de TI ou ao responsável pela segurança da informação, para que as medidas corretivas apropriadas possam ser tomadas.

## 5.13 Mesa Limpa

1. **Conceito de Mesa Limpa:** A política de Mesa Limpa visa reduzir o risco de acesso não autorizado, perda ou danos a informações confidenciais. Colaboradores devem assegurar que todos os documentos sensíveis, dispositivos móveis e mídias removíveis sejam guardados de forma segura quando não estiverem em uso ou quando deixarem seu local de trabalho.

2. **Implementação Prática:** A prática de manter uma mesa limpa inclui não apenas a organização física do espaço de trabalho, mas também a gestão adequada de documentos impressos e eletrônicos. Documentos confidenciais devem

ser armazenados em armários trancados e dispositivos digitais devem ser protegidos por senha ou autenticação biométrica.

3. **Monitoramento e Cumprimento:** Gestores e a equipe de segurança da informação podem vir a realizar inspeções periódicas para assegurar o cumprimento da política de Mesa Limpa. Violações desta política serão tratadas de acordo com os procedimentos disciplinares da empresa.

4. **Reflexos no Ambiente de Trabalho:** Uma política efetiva de Mesa Limpa contribui não apenas para a segurança da informação, mas também para a criação de um ambiente de trabalho mais organizado, eficiente e profissional.

## 5.14 Tela Limpa

1. **Propósito da Política de Tela Limpa:** A política de Tela Limpa visa prevenir a visualização não autorizada de informações confidenciais. Colaboradores devem bloquear suas estações de trabalho, laptops e dispositivos móveis sempre que estes não estiverem em uso.

2. **Implementação:** O bloqueio de tela deve ser automático após um período de inatividade, além da possibilidade de ativação manual pelo usuário. A utilização de senhas seguras é mandatória, e, quando possível, a utilização de autenticação de múltiplos fatores.

3. **Monitoramento e Cumprimento:** Gestores e a equipe de segurança da informação podem vir a realizar inspeções periódicas para assegurar o cumprimento da política de Tela Limpa. Violações desta política serão tratadas de acordo com o procedimento de aplicação de medida disciplinar da empresa.

4. **Cultura de Segurança:** A adoção da política de Tela Limpa deve ser parte integrante da cultura de segurança da empresa, refletindo o compromisso de todos com a proteção das informações.

## 5.15 BYOD (Bring Your Own Device)

1. **Bring Your Own Device:** Os colaboradores da empresa podem ter a oportunidade de usar seus dispositivos eletrônicos pessoais para fins de trabalho quando autorizados pelo gestor da área. Os dispositivos eletrônicos pessoais incluem celulares, smartphones, tablets, laptops e computadores pessoais.

2. **Protocolo do Dispositivo Virtual (Arlequim):** Para garantir a segurança das informações da empresa, os colaboradores autorizados precisam ter um software antivírus, que será instalado pelo departamento de TI da empresa antes de usar o dispositivo Arlequim para fins de trabalho. É proibido fazer qualquer modificação no hardware ou software do dispositivo além das atualizações de instalação autorizadas e de rotina, a menos que seja aprovado pela Tl O bloqueio de tela deve ser automático após um período de inatividade, além da possibilidade de ativação manual pelo usuário. A utilização de senhas seguras e, quando possível, de autenticação de múltiplos fatores é mandatória.

3. **Restrições e Limites:** Os colaboradores cujos dispositivos pessoais tenham capacidade de câmera, vídeo ou gravação devem utilizar essas funções para desenvolvimento da sua atividade dentro da empresa e espera-se que os colaboradores exerçam a mesma discrição no uso de seus dispositivos pessoais que é esperado para o uso de dispositivos da empresa. As políticas da Arlequim relativas a assédio, discriminação, retaliação, segredos comerciais, informações confidenciais e ética se aplicam ao uso de dispositivos pessoais por colaboradores para atividades relacionadas ao trabalho

4. **Monitoramento e Cumprimento:** A empresa reserva-se o direito de revisar ou reter dados pessoais e relacionados à empresa em dispositivos pessoais ou liberar os dados para agências governamentais ou terceiros durante uma investigação ou litígio. Além disso, nenhum colaborador pode desativar conscientemente qualquer software ou sistema de rede identificado como uma ferramenta de monitoramento.

5. **Segurança**: Espera-se que os colaboradores sigam as leis e regulamentos locais, estaduais e federais aplicáveis em relação ao uso de dispositivos eletrônicos em todos os momentos. Os colaboradores têm a obrigação de proteger os dispositivos pessoais usados para fins relacionados ao trabalho contra perda, dano ou roubo, devendo notificar imediatamente o departamento de TI caso seu dispositivo seja perdido, roubado ou danificado. Em nenhuma hipótese a empresa será responsável pelo equipamento perdido, roubado, danificado ou furtado. O colaborador é o único responsável pelo custo de substituição do dispositivo.

6. Mediante pedido de demissão ou rescisão do contrato de trabalho / prestação de serviço, ou a qualquer momento, o colaborador pode ser solicitado a apresentar o dispositivo pessoal para inspeção. Todos os dados da empresa em dispositivos pessoais serão removidos pelo departamento de TI após a rescisão do contrato de trabalho / prestação de serviço.

## 5.16 Utilização Profissional dos Recursos de TI

1. **Uso Adequado dos Recursos:** Os recursos de TI fornecidos pela empresa são destinados exclusivamente para fins profissionais. O uso deve estar alinhado com as metas e objetivos da empresa, evitando atividades que possam comprometer a segurança, estratégia ou a eficiência operacional.

2. **Restrições e Limites:** Atividades como a instalação de software não autorizado, o uso de recursos de TI para fins ilegais ou antiéticos, e o acesso a sites inseguros ou inapropriados são estritamente proibidos. Também não é permitido enviar informações confidenciais ou restritas para terceiros, sem a autorização.

3. **Monitoramento e Auditoria:** O uso dos recursos de TI é sujeito a monitoramento e auditoria. Os colaboradores devem estar cientes de que a empresa reserva o direito de monitorar a utilização dos recursos de TI para garantir o cumprimento das políticas.

4. **Responsabilidade do Usuário:** Cada colaborador é responsável por qualquer atividade realizada com seus recursos de TI. A negligência no uso desses recursos pode resultar em consequências disciplinares e, em casos graves, na adoção de medidas legais.

5. **Segurança e Manutenção:** Os colaboradores devem seguir as orientações do departamento de TI para a segurança e manutenção dos recursos de TI, incluindo atualizações de software, atualização de senhas e medidas de segurança cibernética.

## 5.17 Regras de Utilização dos Recursos de TI

1. **Definição e Alcance:** As regras de utilização dos recursos de TI estabelecem diretrizes claras para o uso apropriado de computadores, dispositivos móveis, redes e software. Estas regras aplicam-se a todos os colaboradores, contratados e terceiros que utilizem os recursos de TI da empresa.

2. **Uso Permitido e Restrições:** Os recursos de TI devem ser utilizados exclusivamente para fins relacionados ao trabalho. Atividades proibidas incluem, mas não se limitam a instalação de software não autorizado, o acesso a sites inapropriados e a realização de atividades que possam prejudicar a infraestrutura de TI ou à Empresa.

3. **Segurança e Prevenção:** Os usuários devem tomar precauções para evitar a exposição de sistemas e dados a riscos de segurança. Isso inclui manter os sistemas operacionais e aplicativos atualizados e evitar a abertura de anexos ou links suspeitos.

4. **Responsabilidade do Usuário:** Cada colaborador é responsável pelo uso adequado dos recursos de TI alocados a ele. Violações das regras de utilização podem resultar na aplicação de medidas disciplinares, incluindo a suspensão do acesso aos recursos de TI, até o desligamento.

5. **Monitoramento e Conformidade:** A empresa reserva-se o direito de monitorar o uso dos recursos de TI para garantir a conformidade com as políticas estabelecidas. Este monitoramento será realizado respeitando as leis aplicáveis e a privacidade dos colaboradores.

## 5.18 Cuidados com as Senhas e Responsabilidade

1. **Importância das Senhas:** Uma senha forte é crucial para a segurança da informação. Os colaboradores devem estar cientes da importância de criar e manter senhas seguras.

2. **Criação de Senhas Fortes:** As senhas devem conter uma combinação de letras, números e símbolos e não devem incluir informações facilmente acessíveis, como datas de aniversário ou nomes de familiares.

3. **Manutenção da Confidencialidade:** A confidencialidade da senha é responsabilidade pessoal de cada colaborador. Elas nunca devem ser anotadas ou compartilhadas.

4. **Consequências do Uso Inadequado:** O uso inadequado ou negligente das senhas pode resultar em acesso não autorizado a informações confidenciais e sensíveis, colocando em risco a segurança e o negócio da empresa.

## 5.19 Utilização de Softwares

1. **Software Autorizado:** Apenas softwares licenciados e aprovados pela empresa podem ser instalados e utilizados nos dispositivos de TI. A instalação de software não autorizado é estritamente proibida.

2. **Licenciamento e Conformidade:** A empresa é responsável por garantir que todos os softwares utilizados estejam devidamente licenciados, em conformidade com as leis de direitos autorais e que sejam utilizados respeitando seus contratos.

3. **Atualizações e Patches de Segurança:** Os softwares devem ser mantidos atualizados, com a aplicação regular de patches de segurança para proteger contra vulnerabilidades conhecidas.

4. **Auditoria e Inventário de Software:** Deve ser mantido um inventário atualizado de todos os softwares instalados, e auditorias regulares devem ser realizadas para garantir a conformidade e a integridade do ambiente de software.

5. **Remoção de Software Não Autorizado:** Uma vez identificado em auditoria, software não autorizado ou irregular, este deverá ser removido imediatamente para garantir a segurança e a conformidade da Empresa.

## 5.20 Proteção contra Vírus de Computador

1. **Software Antivírus:** O uso de software antivírus é obrigatório em todos os dispositivos que acessam a rede da empresa, exceto BYOD. O software antivírus deve ser mantido atualizado para garantir a máxima eficácia.

2. **Prevenção e Detecção:** Além do antivírus, outras medidas de prevenção, como firewalls e sistemas de detecção de intrusão, devem ser implementadas para proteger contra malware e ataques cibernéticos.

3. **Ação em Caso de Infecção:** Em caso de detecção de vírus ou malware, o dispositivo afetado deve ser imediatamente desconectado da rede e reportado ao departamento de TI para ação corretiva.

## 5.21 Utilização da Internet

1. **Finalidade e Limites:** O acesso à Internet nos dispositivos da empresa deve ser usado primordialmente para fins profissionais. Atividades não relacionadas ao trabalho devem ser limitadas e não devem interferir nas responsabilidades profissionais.

2. **Sites Proibidos e Perigosos:** É estritamente proibido acessar sites que contenham material ofensivo, ilegal, ou que representem uma ameaça à segurança, como páginas de phishing ou que contenham malwares.

3. **Segurança Online:** Os colaboradores devem estar atentos aos riscos associados ao uso da Internet, incluindo golpes, engenharia social e ataques de phishing. A conscientização e treinamentos regulares sobre segurança online são essenciais.

4. **Monitoramento e Auditoria:** O uso da Internet pelos colaboradores pode ser monitorado e auditado para garantir a conformidade com as políticas da empresa. Este monitoramento será conduzido em conformidade com as leis de privacidade aplicáveis e nos termos desta Política.

5. **Uso Responsável:** Todos os colaboradores devem usar a Internet de maneira responsável, evitando sobrecarregar a rede com atividades desnecessárias e mantendo a segurança dos sistemas e dados da empresa.

## 5.22 Rede WiFi

1. **Segurança da Rede:** As redes WiFi da empresa devem ser seguras, utilizando criptografia forte e medidas de autenticação para controlar o acesso. Redes não seguras ou públicas devem ser evitadas para atividades de trabalho.

2. **Acesso e Uso:** O acesso à rede WiFi corporativa é restrito a colaboradores e visitantes autorizados. O uso indevido da rede, incluindo atividades não autorizadas ou prejudiciais, é proibido.

3. **Configuração e Manutenção:** A rede WiFi deve ser configurada e mantida pela equipe de TI, assegurando que as configurações de segurança estejam sempre atualizadas para proteger contra vulnerabilidades.

4. **Monitoramento da Rede:** A utilização da rede WiFi será monitorada para detectar atividades suspeitas, uso indevido ou tentativas de acesso não autorizado.

## 5.23 Demais Recursos de TI

1. **Abrangência e Responsabilidade:** Esta seção abrange todos os outros recursos de TI não especificamente mencionados anteriormente, incluindo hardware, software, periféricos e serviços relacionados. Todos os colaboradores são responsáveis pelo uso adequado e seguro desses recursos.

2. **Manutenção e Atualizações:** A manutenção regular e as atualizações de todos os recursos de TI são essenciais para garantir a segurança e eficiência operacional. Os colaboradores devem seguir as orientações da equipe de TI para a manutenção desses recursos.

3. **Uso Apropriado e Eficiente:** Os recursos de TI devem ser usados de maneira eficiente e adequada, evitando desperdício e garantindo que sejam utilizados para os fins pretendidos.

4. **Relato de Problemas e Incidentes:** Qualquer problema, defeito ou incidente relacionado aos recursos de TI deve ser imediatamente reportado à equipe de TI para ação corretiva.

5. **Conformidade com as Políticas:** O uso de todos os recursos de TI deve estar em conformidade com as políticas e procedimentos da empresa, incluindo as diretrizes de segurança da informação.

## 5.24 Alimentos, Bebidas e Afins

1. **Restrições e Cuidados:** É proibido o consumo de alimentos e bebidas nas áreas onde estão localizados os equipamentos de TI para evitar danos aos dispositivos e manter a limpeza e higiene do ambiente de trabalho.

2. **Áreas Designadas:** Colaboradores devem utilizar as áreas designadas, como refeitórios ou áreas de descanso, para o consumo de alimentos e bebidas e respeitar a política de uso das copas.

3. **Limpeza e Organização:** As áreas de trabalho devem ser mantidas limpas e organizadas. Qualquer derramamento ou sujeira deve ser imediatamente limpo para evitar danos aos equipamentos e manter um ambiente de trabalho agradável.

4. **Cumprimento das Regras:** A violação das regras relativas ao consumo de alimentos e bebidas pode resultar em medidas disciplinares, pois tais ações podem comprometer a integridade dos recursos de TI.

## 5.25 Teletrabalho

1. **Segurança no Teletrabalho:** Os colaboradores que trabalham remotamente devem seguir as mesmas políticas de segurança da informação aplicadas no escritório, incluindo a proteção de dados, o uso seguro da Internet e a proteção de dispositivos.

2. **Ambiente de Trabalho Seguro:** É responsabilidade do colaborador garantir que o ambiente de teletrabalho seja seguro e livre de riscos que possam comprometer a segurança da informação.

3. **Recursos:** Os colaboradores devem utilizar os recursos fornecidos pela empresa para o trabalho remoto e garantir que esses recursos sejam utilizados de forma segura e conforme as políticas da empresa.

4. **Comunicação e Relatório de Incidentes:** Os colaboradores em teletrabalho devem manter uma comunicação regular com a equipe e reportar imediatamente qualquer incidente de segurança da informação.

## 5.26 Visitantes

1. **Controle de Acesso:** O acesso de visitantes às instalações da empresa deve ser controlado e monitorado. Visitantes devem ser acompanhados por um colaborador autorizado em todas as áreas de acesso restrito.

2. **Política de Não Divulgação:** Visitantes podem ser solicitados a assinar uma política de não divulgação ou acordo de confidencialidade, especialmente ao acessar áreas onde informações sensíveis são manipuladas.

3. **Identificação e Registro:** Todos os visitantes devem ser registrados na recepção e usar identificação visível durante sua estadia nas instalações da empresa.

4. **Restrições de Acesso:** O acesso dos visitantes aos recursos de TI da empresa deve ser restrito e monitorado, garantindo que não tenham acesso a informações confidenciais ou sistemas críticos.

## 5.27 Clientes

1. **Proteção de Dados dos Clientes:** É essencial garantir a proteção dos dados pessoais e confidenciais dos clientes, em conformidade com as leis e regulamentos aplicáveis, como a LGPD e o Marco Civil.

2. **Transparência nas Operações:** Deve haver transparência nas operações que envolvem dados dos clientes, proporcionando-lhes clareza sobre a utilização, finalidade, base legal e o armazenamento de suas informações.

3. **Atendimento a Requisições e Direitos dos Clientes:** A empresa deve estar preparada para atender prontamente a solicitações de clientes relacionadas aos seus dados, como pedidos de acesso, retificação ou exclusão, respeitadas as ressalvas legais.

4. **Resposta a Incidentes Envolvendo Clientes:** Em caso de incidentes de segurança que afetem dados de clientes, a empresa através de seu DPO, deve ter um plano de comunicação e resposta eficaz para minimizar o impacto e restaurar a confiança.

5. **DPO**: Manter em seus Canais de comunicação os dados atualizados de seu Encarregado de Dados, para fins de exercício dos direitos dos usuários e contato das Autoridades Competentes.

## 5.28 Terceirização de Serviços

1. **Avaliação de Fornecedores:** Ao terceirizar serviços, é crucial avaliar a capacidade do fornecedor de cumprir com os requisitos de segurança da informação. Isso inclui a realização de auditorias e análise de sua infraestrutura e práticas de segurança.

2. **Acordos de Nível de Serviço (SLAs):** Os SLAs devem incluir cláusulas específicas de segurança da informação, garantindo que os fornecedores mantenham um nível de segurança compatível com as políticas da empresa.

3. **Monitoramento e Gestão de Fornecedores:** A empresa deve monitorar continuamente o desempenho dos fornecedores em relação à segurança da informação e gerenciar ativamente essas relações para assegurar a conformidade.

4. **Resposta a Incidentes com Fornecedores:** Deve haver planos claros para a resposta a incidentes de segurança que envolvam fornecedores terceirizados, incluindo procedimentos de comunicação e escalonamento.

5. **Revisão e Atualização de Contratos:** Os contratos com fornecedores devem ser revisados e atualizados regularmente para refletir as mudanças nas exigências de segurança e regulamentações.

## 5.29 Auditoria

1. **Equipe Interna de Auditoria:** A empresa deve ter uma equipe interna dedicada à realização de auditorias regulares de segurança da informação. Esta equipe deve ter conhecimento e habilidades especializadas em práticas de segurança da informação e auditoria.

2. **Auditorias Externas:** Além das auditorias internas, a empresa deve contratar periodicamente auditores externos independentes para realizar uma análise imparcial das práticas de segurança da informação.

3. **Responsabilidades e Autoridade:** Os responsáveis pela auditoria devem ter autoridade clara e responsabilidade definida para realizar auditorias, reportar descobertas e recomendar melhorias.

4. **Formação e Certificações:** Os membros da equipe de auditoria devem possuir formação adequada e, idealmente, certificações profissionais em auditoria de sistemas de informação.

5. **Continuidade e Melhoria:** A função de auditoria deve ser uma atividade contínua, com foco na melhoria constante das práticas de segurança da informação da empresa. Feedback e recomendações da auditoria devem ser prontamente implementados para reforçar a postura de segurança.

## 5.30 Auditoria e Monitoramento

1. **Importância da Auditoria:** A auditoria regular dos sistemas de TI é crucial para garantir a conformidade com as políticas de segurança da informação e identificar áreas de melhoria. Auditorias internas e externas devem ser realizadas para avaliar a eficácia das medidas de segurança.

2. **Monitoramento Contínuo:** O monitoramento contínuo dos sistemas de TI permite a detecção rápida de atividades suspeitas ou anormais. Ferramentas de monitoramento devem ser utilizadas para rastrear o uso de recursos de TI, acessos a sistemas críticos e tráfego de rede.

3. **Relatórios e Análise:** Os dados coletados durante o monitoramento devem ser analisados para identificar tendências, vulnerabilidades e ameaças potenciais. Relatórios detalhados devem ser gerados e revisados regularmente pela equipe de segurança da informação.

4. **Resposta a Incidentes:** Em caso de detecção de uma ameaça ou violação, deve haver um plano de resposta a incidentes claramente definido para mitigar o impacto e restaurar a segurança.

5. **Melhoria Contínua:** Os resultados das auditorias e do monitoramento devem ser utilizados para aprimorar continuamente as políticas e práticas de segurança da informação.

## 5.31 Plano de Resposta a Incidentes de Segurança

1. **Estrutura do Plano de Resposta:** O plano de resposta a incidentes de segurança da informação deve estabelecer procedimentos claros para responder a incidentes de segurança, minimizando impactos e recuperando a normalidade operacional o mais rápido possível.

2. **Equipe de Resposta a Incidentes:** Deve existir uma equipe dedicada, treinada e equipada para responder a incidentes de segurança. Esta equipe deve ter responsabilidades e autoridades claramente definidas para agir em caso de incidentes.

3. **Detecção e Relato de Incidentes:** O plano deve incluir métodos para a rápida detecção de incidentes de segurança e procedimentos para o relato imediato destes incidentes à equipe de resposta.

4. **Análise e Contenção:** Após a detecção de um incidente, a equipe de resposta deve analisá-lo para determinar sua gravidade e implementar medidas para contê-lo e minimizar danos.

5. **Recuperação e Aprendizado:** O plano deve estabelecer procedimentos para a recuperação dos sistemas afetados e para a aprendizagem com o incidente, de forma a melhorar continuamente as estratégias de segurança da informação.

## 5.32 Requisitos Legais e Normativos

1. **Marco Civil da Internet**

   1.1. **Conformidade com o Marco Civil**: A PSI deve estar em conformidade com o Marco Civil da Internet, legislação brasileira que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

   1.2. **Proteção da Privacidade:** O Marco Civil exige a proteção da privacidade dos usuários da Internet, o que implica em medidas rigorosas de segurança da informação para proteger dados pessoais e comunicações privadas.

   1.3. **Responsabilidade por Dados Armazenados:** De acordo com o Marco Civil, a empresa é responsável pela segurança dos dados que armazena, devendo adotar medidas técnicas adequadas para protegê-los.

   1.4. **Resposta a Requisições Legais:** A empresa deve estar preparada para responder a requisições legais de dados, conforme estabelecido pelo Marco Civil, de forma a cumprir com as obrigações legais sem violar a privacidade dos usuários.

   1.5. **Transparência e Informação aos Usuários:** É necessário manter transparência sobre as práticas de coleta, uso e armazenamento de dados, informando claramente aos usuários sobre essas práticas.

2. **LGPD (Lei Geral de Proteção de Dados)**

   2.1. **Adesão à LGPD:** A PSI deve estar alinhada com os requisitos da LGPD, que regulamenta o tratamento de dados pessoais no Brasil, garantindo a proteção dos direitos fundamentais de liberdade e de privacidade.

   2.2. **Consentimento e Transparência:** A LGPD exige o consentimento claro dos indivíduos para o tratamento de seus dados pessoais, e a empresa deve garantir transparência quanto ao uso destes dados.

**2.3. Direito dos Titulares de Dados:** A empresa deve assegurar e facilitar o exercício dos direitos dos titulares de dados, como acesso, correção, exclusão ou portabilidade de seus dados pessoais.

**2.4. Registro e Relato de Incidentes:** A LGPD exige que a empresa mantenha registro de operações de tratamento de dados e notifique as autoridades e titulares em caso de incidentes de segurança que resultem em risco ou dano relevante aos titulares.

**2.5. Encarregado de Dados (DPO):** A empresa deve designar um Encarregado de Dados (Data Protection Officer - DPO) responsável por assegurar a conformidade com a LGPD e ser um ponto de contato com os titulares e a autoridade nacional.

**3. ISO/IEC 27001:2022**

**3.1. Implementação da ISO 27001:** A empresa deve implementar um Sistema de Gestão de Segurança da Informação (SGSI) conforme a norma ISO/IEC 27001:2022, que estabelece requisitos para a gestão de segurança da informação.

**3.2. Avaliação de Risco e Tratamento:** A norma exige uma abordagem baseada em risco para a segurança da informação, exigindo a identificação, análise e tratamento de riscos de segurança da informação.

**3.3. Políticas e Procedimentos**: A ISO 27001 requer a definição de políticas e procedimentos claros de segurança da informação, que devem ser comunicados a todos os colaboradores e partes interessadas.

**3.4. Revisão e Melhoria Contínua:** A norma enfatiza a necessidade de revisão contínua e melhoria do SGSI, garantindo que o sistema permaneça eficaz diante das mudanças nas ameaças e no ambiente de negócios.

**3.5. Auditoria e Certificação:** A empresa pode buscar a certificação ISO 27001 para demonstrar conformidade com a norma, o que envolve auditorias regulares por um organismo de certificação independente.

**4. ISO/IEC 27701:2019**

**4.1. Extensão da ISO 27001 para Privacidade**: A ISO/IEC 27701:2019 é uma extensão da ISO 27001, focada em requisitos específicos para o gerenciamento de informações de privacidade.

**4.2. Integrando Privacidade no SGSI:** A norma orienta sobre como integrar práticas de proteção de privacidade no SGSI existente, alinhando segurança da informação e gestão de privacidade.

**4.3. Controles de Privacidade:** A ISO 27701 específica controles adicionais e orientações para a gestão de PII (Personal Identifiable Information), complementando os controles de segurança da ISO 27001.

**4.4. Interoperabilidade com Regulamentos de Privacidade:** A norma é projetada para ajudar as organizações a se alinharem com regulamentos de privacidade globais, como GDPR e LGPD, através da implementação de práticas consistentes de privacidade.

**4.5. Melhoria e Revisão Contínua:** Assim como a ISO 27001, a ISO 27701 enfatiza a necessidade de revisão e melhoria contínuas das práticas de privacidade, adaptando-se às mudanças nas leis, tecnologias e no ambiente de negócios.