IntegraSolução®

FÁBRICA DE SOFTWARE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Controle: A.5.1. ISO/IEC 27001:2022

Página 01 de 32

Versão: 01/2025

Classificação: Interno

Elaboração	Revisão	Aprovação
Assessoria Externa	Assessoria Externa / Alta Gestão	Alta Gestão
Data	**Data**	**Data**
10/06/2025	13/06/2025	13/08/2025

Sumário

Introdução

Em um cenário cada vez mais digital e interconectado, a gestão eficiente e segura das informações torna-se um imperativo essencial para as organizações. No contexto específico de um sistema para gestão de clínicas e consultórios médicos, onde trata se diariamente com uma vasta gama de dados sensíveis e confidenciais, a implementação de uma política de segurança da informação é crucial para assegurar a confiabilidade, integridade e confidencialidade dessas informações.

A segurança da informação não é apenas uma questão de conformidade com normas regulatórias, mas uma salvaguarda estratégica para a reputação e continuidade do negócio. Vivenciamos um ambiente no qual as ameaças cibernéticas evoluem constantemente, e a crescente dependência de sistemas informatizados demanda uma abordagem proativa para a proteção de dados.

Objetivo desta Política

O objetivo primordial desta Política de Segurança da Informação é estabelecer diretrizes claras e abrangentes para a proteção de todos os ativos de informação sob a responsabilidade da GestãoDS. Buscando promover uma cultura organizacional que reconheça a importância da segurança da informação em todas as atividades, desde a coleta inicial até o processamento e armazenamento, garantindo a transparência, a ética e a conformidade com as leis, regulamentações aplicáveis e normas, como a Lei 13.709/2018 (LGPD), normas ISO/IEC 27001/2022 e o conjunto de requisitos técnicos de Segurança da Informação proposto pela Sociedade Brasileira de Informática em Saúde (SBIS) para o Manual de Certificação de Sistemas de Registro Eletrônico em Saúde (S-RES).

Ao implementar esta política, almejamos

- Proteção de Dados Sensíveis: Garantir a confidencialidade e integridade dos dados sensíveis dos clientes, parceiros e colaboradores, minimizando o risco de divulgação não autorizada.

- Resposta Eficiente a Incidentes: Desenvolver procedimentos robustos para identificar, avaliar e responder rapidamente a incidentes de segurança da informação, minimizando danos e interrupções.
- Conscientização e Treinamento: Promover a conscientização e treinamento contínuos para todos os colaboradores, capacitando-os a reconhecer e mitigar ameaças à segurança da informação.
- Compliance Legal: Assegurar o cumprimento das leis e regulamentações pertinentes relacionadas à segurança da informação, protegendo a reputação e evitando possíveis implicações legais.

Ao adotarmos e internalizarmos esses princípios, fortalecemos não apenas a segurança de nossas operações, mas também a confiança depositada em nós por nossos clientes e parceiros.

A colaboração de cada membro desta organização é fundamental para o sucesso dessa iniciativa, e a adesão a esta política é um compromisso conjunto para preservar a integridade e confiabilidade das informações que tratamos.

Escopo

O escopo desta Política de Segurança da Informação abrange todos os aspectos relacionados à gestão, manuseio e proteção de informações dentro da organização. Essa política é aplicável a todos os colaboradores, prestadores de serviço e demais partes que tenham acesso a dados e sistemas vinculados às atividades da organização. Este escopo inclui, mas não se limita a:

- **Informações do Cliente:** Dados pessoais dos clientes, incluindo informações de contato, histórico financeiro, e quaisquer dados relacionados às transações e acordos de pagamento.
- **Prontuários Médicos:** Dados pessoais de pacientes, dados sensíveis de pacientes, atendidos pelos nossos clientes, incluindo informações de contato, histórico médico, atendimentos, agendamentos e quaisquer dados relacionados às transações e acordos de pagamento.

- **Informações Financeiras:** Dados relacionados a transações financeiras, pagamentos, saldos devedores, e quaisquer outros detalhes financeiros relevantes.
- **Sistemas e Aplicações:** Todos os sistemas de TI, softwares, e plataformas utilizadas para processamento de dados, comunicação e armazenamento de informações.
- **Comunicações:** Qualquer forma de comunicação, seja ela interna ou externa, que envolva a transmissão de informações relacionadas às atividades da organização.
- **Documentação Contratual:** Contratos, acordos, e qualquer outra documentação legal que contenha informações relevantes às operações.
- **Dispositivos Móveis:** Dispositivos móveis utilizados para acessar, armazenar ou processar informações da organização, incluindo smartphones, tablets, e laptops.
- **Acesso Físico:** Medidas de segurança física para proteger instalações, equipamentos e documentos que contenham informações sensíveis.
- **Treinamento e Conscientização:** Programas de treinamento e conscientização destinados a todos os colaboradores para promover a segurança da informação.
- **Gestão de Incidentes:** Procedimentos para identificar, relatar e responder a incidentes de segurança da informação, garantindo uma abordagem consistente e eficaz.
- **Backup e Recuperação:** Processos para realizar backups regulares e garantir a rápida recuperação de dados em caso de perda ou incidente.
- **Monitoramento e Auditoria:** Mecanismos de monitoramento e auditoria para avaliar a eficácia das medidas de segurança implementadas e identificar possíveis áreas de melhoria.

Este escopo é aberto a revisões periódicas para garantir que permaneça alinhado com as práticas e requisitos de segurança da informação em constante evolução. O compromisso com a segurança da informação é vital para a integridade e reputação da organização, sendo responsabilidade de todos os envolvidos a adesão a esta política e seu escopo abrangente.

Responsabilidades

Direção e Alta Administração

- Estabelecer um ambiente propício à segurança da informação.

- Designar responsáveis pela supervisão e implementação das diretrizes de segurança.
- Assegurar recursos adequados para a implementação eficaz da política.

Gerenciamento de TI

- Implementar e manter controles de segurança em sistemas e redes.
- Monitorar atividades suspeitas e realizar auditorias regulares.
- Manter atualizados os sistemas de proteção contra ameaças cibernéticas.

Colaboradores

- Conhecer e seguir as políticas e procedimentos de segurança da informação.
- Reportar imediatamente quaisquer incidentes de segurança ou práticas inadequadas.
- Participar de treinamentos regulares de conscientização sobre segurança.

Departamento Comercial e Atendimento

- Proteger informações dos clientes durante o manuseio, processamento e armazenamento.
- Garantir que documentos contratuais sejam armazenados e manipulados com segurança.
- Implementar controles de acesso adequados para informações sensíveis.

Recursos Humanos

- Conduzir verificações de antecedentes antes da contratação.
- Garantir que os funcionários tenham acesso apenas às informações necessárias para suas funções.
- Fornecer treinamento inicial e contínuo sobre práticas seguras de manuseio de informações.

Departamento Jurídico

- Assegurar que as práticas comerciais e operacionais estejam em conformidade com as leis e regulamentações aplicáveis.
- Colaborar na elaboração de cláusulas contratuais relacionadas à segurança da informação.

Segurança Física

- Implementar medidas para controlar o acesso físico às instalações.
- Garantir a segurança de documentos físicos que contenham informações sensíveis.

Responsável pelo Treinamento

- Desenvolver e conduzir programas de treinamento de conscientização sobre segurança.
- Manter materiais de treinamento atualizados conforme as ameaças evoluem.

Auditoria Interna

- Realizar auditorias regulares para avaliar a conformidade com a política.
- Identificar e relatar áreas de não conformidade, propondo melhorias.

Comitê de Segurança da Informação

- Coordenar esforços para implementar e manter a política.
- Revisar regularmente a eficácia das medidas de segurança.

Ao designar responsabilidades claras para diferentes áreas e funções, buscamos criar uma cultura organizacional que valorize e integre a segurança da informação em todas as operações da GestãoDS. Cada membro da equipe desempenha um papel fundamental na preservação da confidencialidade, integridade e disponibilidade das informações sob nossa responsabilidade.

Classificação das Informações

A classificação da sensibilidade das informações da organização é essencial para direcionar medidas de segurança apropriadas e garantir a proteção adequada dos dados.

Informações Públicas

- Dados que estão disponíveis publicamente ou que não são confidenciais.
- Exemplos: Informações de contato geral, informações publicamente disponíveis sobre empresas.

Informações Internas

- Dados que são relevantes para as operações internas, mas que não são altamente confidenciais.
- Exemplos: Diretórios internos, informações de contato de funcionários.

Informações do Cliente (Não Sensíveis)

- Dados de clientes que não são altamente sensíveis e podem ser compartilhados com maior flexibilidade.
- Exemplos: Informações de contato básicas, histórico de transações não delicadas.

Informações do Cliente (Sensíveis)

- Dados mais sensíveis relacionados aos clientes, que requerem um controle mais rigoroso.
- Exemplo: Dados de saúde, prontuários médico.

Informações Financeiras Confidenciais

- Dados financeiros altamente sensíveis que exigem proteção rigorosa.
- Exemplos: Números de contas bancárias, detalhes de cartões de crédito.

Informações Contratuais

- Dados contidos em contratos e acordos que precisam de proteção especial.
- Exemplos: Termos contratuais, detalhes de acordos de pagamento.

Informações Jurídicas e Regulatórias

- Dados relacionados a assuntos legais e regulatórios que requerem conformidade estrita.

- Exemplos: Comunicações legais, documentação de conformidade regulatória.

Informações de Cobrança em Andamento

- Dados relacionados a processos de cobrança ativos que precisam de confidencialidade.
- Exemplos: Comunicações de cobrança, informações de negociação em andamento.

Informações Pessoais dos Funcionários

- Dados pessoais dos colaboradores que requerem proteção.
- Exemplos: Informações de RH, registros de empregados.

Informações Críticas para o Negócio

- Dados cuja perda, divulgação ou acesso não autorizado pode ter um impacto significativo nos negócios.
- Exemplos: Estratégias de cobrança, dados de desempenho financeiro, segredos comerciais e propriedade intelectual.

Acesso à informação

Para controlar o acesso às informações, baseando-se nas normas ISO/IEC 27001, é fundamental implementar regras e procedimentos claros que garantam a confidencialidade, integridade e disponibilidade dos dados. A norma ISO/IEC 27001 define uma abordagem de Sistema de Gestão de Segurança da Informação (SGSI).

Regras de Controle de Acesso

- Identificação e Autenticação:
  - Cada usuário deve ser devidamente identificado antes de ser concedido acesso ao sistema.
  - Utilizar métodos robustos de autenticação, como senhas seguras, autenticação de dois fatores, ou biometria, dependendo do nível de sensibilidade dos dados.

- Autorização de Acesso:
    - Atribuir permissões de acesso com base nos princípios do "princípio do privilégio mínimo" – cada usuário deve ter acesso apenas às informações necessárias para desempenhar suas funções.
    - Utilizar grupos de usuários para facilitar a gestão e a atribuição consistente de permissões.

- Monitoramento de Acesso:
    - Implementar ferramentas de monitoramento para registrar atividades de acesso.

- Revogação de Acesso:
    - Desativar ou ajustar imediatamente as permissões de acesso quando um usuário muda de função ou deixa a organização.
    - Implementar um processo formal para revisar regularmente as permissões de acesso e ajustá-las conforme necessário.

Procedimentos de Controle de Acesso

- Política de Controle de Acesso:
    - Desenvolver uma política abrangente que aborde a identificação, autenticação, autorização e monitoramento de acesso.
    - Garantir que a política esteja alinhada com os objetivos de segurança da informação e seja revisada regularmente.

- Gestão de Contas de Usuário:
    - Estabelecer procedimentos para criar, modificar e desativar contas de usuário de forma segura.
    - Implementar um processo formal de revisão de contas de usuário para garantir que apenas usuários autorizados tenham acesso.

- Proteção de Senhas:
    - Definir requisitos rigorosos para a criação e gerenciamento de senhas.
    - Promover a troca regular de senhas e utilizar técnicas seguras de armazenamento de senhas.

- Treinamento de Conscientização:
    - Fornecer treinamento regular aos usuários sobre práticas seguras de controle de acesso.
    - Educar os usuários sobre a importância de proteger suas credenciais de acesso.

- Avaliação de Riscos:
    - Realizar avaliações regulares de riscos relacionados ao controle de acesso.
    - Utilizar os resultados para ajustar políticas e procedimentos conforme necessário.

- Documentação e Revisão:
    - Documentar todas as regras e procedimentos relacionados ao controle de acesso.
    - Revisar e atualizar a documentação regularmente para refletir mudanças nos sistemas ou nas práticas de segurança.

- Conformidade com a ISO/IEC 27001:
    - Garantir que todos os controles de acesso estejam em conformidade com os requisitos da norma ISO/IEC 27001.
    - Participar de auditorias internas e externas para verificar a eficácia dos controles de acesso implementados.

Proteção de Senhas

Diretrizes para a criação, gerenciamento e proteção de senhas são fundamentais para garantir a segurança da informação em qualquer ambiente.

Complexidade da Senha

- Usar senhas complexas contendo uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.
- Evitar palavras óbvias, sequências numéricas simples ou informações pessoais facilmente identificáveis.

Tamanho da Senha

- Optar por senhas longas, com no mínimo 12 caracteres. Quanto mais longa a senha, mais difícil é quebrá-la.

Evitar Senhas Comuns

- Não utilizar senhas comuns, como "123456" ou "password". Preferir combinações exclusivas e difíceis de adivinhar.

Atualização Regular

- Estabelecer políticas para a troca regular de senhas, por exemplo, a cada 90 dias. Isso reduz o risco de comprometimento da conta ao longo do tempo.

Não Compartilhar Senhas

- Incentivar fortemente que os usuários não compartilhem suas senhas com colegas ou terceiros. Cada usuário deve ter sua própria senha.

Armazenamento Seguro

- Armazenar as senhas de forma segura, utilizando métodos criptográficos adequados. Evitar armazenamento em texto simples.

Autenticação de Dois Fatores (2FA)

- Implementar a autenticação de dois fatores sempre que possível. Isso adiciona uma camada extra de segurança, exigindo uma segunda forma de verificação além da senha.

Monitoramento de Atividades

- Monitorar e registrar as atividades relacionadas a senhas, como tentativas de login mal-sucedidas, para identificar potenciais ameaças.

Treinamento de Usuários

- Fornecer treinamento regular aos usuários sobre práticas seguras de senha, conscientizando-os sobre a importância de manter senhas seguras e protegidas.

Revisão Periódica

- Realizar revisões periódicas das políticas de segurança de senhas para garantir que estejam alinhadas com as melhores práticas atuais e façam as atualizações necessárias conforme a evolução das ameaças.

Gestão de Dispositivos Móveis

A implementação de regras para dispositivos móveis é essencial em uma política de segurança da informação, especialmente considerando a prevalência do uso de smartphones e tablets no ambiente corporativo.

Autenticação Forte

- Exigir autenticação forte, como PINs, senhas complexas ou biometria, para desbloquear dispositivos móveis.

Criptografia de Dados

- Garantir que os dados armazenados nos dispositivos móveis estejam criptografados, impedindo o acesso não autorizado em caso de perda ou roubo.

Política de Atualização

- Estabelecer uma política que incentive ou exija que os dispositivos móveis estejam sempre atualizados com as últimas versões de software e patches de segurança.

Controle de Acesso

- Implementar políticas de controle de acesso para restringir o acesso a dados sensíveis apenas a usuários autorizados. Isso pode envolver o uso de VPNs e autenticação de dois fatores.

Aplicativos Aprovados

- Permitir apenas a instalação de aplicativos aprovados pela organização. A utilização de lojas de aplicativos oficiais pode ajudar a garantir a segurança.

Gestão Remota de Dispositivos

- Adotar soluções de gerenciamento remoto para rastrear, bloquear ou apagar dados de dispositivos perdidos ou roubados, garantindo a proteção das informações corporativas.

Política de Backup

- Estabelecer diretrizes claras para realizar backups regulares dos dados armazenados nos dispositivos móveis, facilitando a recuperação em caso de perda de dados.

Uso de Redes Seguras

- Orientar os usuários a evitar o uso de redes Wi-Fi públicas e a conectar-se apenas a redes seguras, preferencialmente usando VPNs para criptografar a comunicação.

Monitoramento de Atividades

- Implemente ferramentas de monitoramento para rastrear atividades suspeitas nos dispositivos móveis, identificando potenciais ameaças à segurança da informação.

Treinamento de Usuários

- Oferecer treinamentos regulares aos usuários sobre as práticas seguras de uso de dispositivos móveis, destacando os riscos associados e as medidas preventivas.

Política de Perda ou Roubo

- Estabeleça procedimentos claros a serem seguidos em caso de perda ou roubo de um dispositivo, incluindo a notificação imediata à equipe de segurança.

Compliance com Normas e Regulações

- Garantir que a política de dispositivos móveis esteja em conformidade com as normas e regulamentações relevantes da indústria, como o ISO/IEC 27001, LGPD, GDPR, HIPAA, entre outras, dependendo do setor.

Segurança Física

A proteção de instalações físicas e equipamentos da organização é crucial para garantir a integridade, confidencialidade e disponibilidade das informações.

Controle de Acesso

- Implementar um sistema de controle de acesso físico, como cartões de identificação, biometria ou chaves, para restringir o acesso apenas a pessoal autorizado. Considere a segmentação de áreas sensíveis.

Monitoramento por Câmeras

- Câmeras de vigilância em pontos estratégicos para monitorar o acesso às instalações e registrar atividades relevantes. Certifique-se de que as câmeras estejam em locais visíveis para dissuadir comportamentos inadequados.

Iluminação Adequada

- Manter áreas externas e internas bem iluminadas para evitar pontos cegos e reduzir o risco de atividades não autorizadas.

Segurança Física de Equipamentos

- Proteger os equipamentos sensíveis, como servidores e sistemas de armazenamento, em áreas seguras, com controle de acesso restrito. Utilizar racks fechados e gabinetes com fechaduras.

Backup de Energia

- Instalar sistemas de backup de energia, como geradores ou nobreaks, para garantir a continuidade das operações em caso de falhas de energia.

Treinamento de Funcionários

- Fornecer treinamentos regulares aos funcionários sobre procedimentos de segurança, incluindo a importância de manter portas fechadas, não compartilhar informações confidenciais e relatar atividades suspeitas.

Política de Limpeza de Mesas

- Estabelecer uma política rigorosa para garantir que todas as mesas e áreas de trabalho estejam limpas e sem documentos sensíveis quando não estiverem em uso.

Manutenção Regular de Equipamentos

- Manter uma programação de manutenção regular para equipamentos críticos, verificando a integridade física e garantindo atualizações de segurança.

Gestão de Resíduos

- Implementar procedimentos adequados para a eliminação segura de documentos impressos e dispositivos eletrônicos fora de uso, a fim de evitar vazamentos de informações sensíveis.

Política de Visitantes

- Estabelecer regras claras para o acesso de visitantes, exigindo identificação e acompanhamento durante a permanência nas instalações.

Monitoramento e Auditoria

A monitorização de atividades e auditorias de segurança são componentes essenciais de uma política de segurança da informação. Esses procedimentos ajudam a identificar possíveis ameaças, garantir a conformidade com as políticas estabelecidas e manter um ambiente seguro.

Implementação de Ferramentas de Monitoramento

- Utilizar ferramentas de monitoramento de segurança para rastrear atividades em sistemas, redes e servidores. Isso inclui logs de eventos, sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS).

Registro e Análise de Logs

- Registrar eventos significativos em logs de sistemas e aplicar análises regulares para identificar padrões incomuns ou atividades suspeitas que possam indicar uma violação de segurança.

Monitoramento de Acesso de Usuários

- Acompanhar o acesso de usuários a sistemas e dados sensíveis. Estar atento a atividades fora do padrão, como acessos fora do horário comercial ou acessos a áreas não autorizadas.

Auditorias Periódicas de Contas de Usuários

- Realizar auditorias regulares nas contas de usuários para garantir que apenas as pessoas autorizadas tenham acesso a sistemas e dados relevantes. Revisar e remover contas inativas ou desnecessárias.

Testes de Penetração

- Realizar testes de penetração regulares para identificar vulnerabilidades em sistemas e redes. Isso ajuda a antecipar possíveis brechas de segurança e fortalecer as defesas.

Monitoramento de Tráfego de Rede

- Analisar o tráfego de rede em busca de padrões suspeitos ou tráfego malicioso. Implementar sistemas de detecção de anomalias para identificar atividades incomuns.

Revisão de Configurações de Sistemas

- Regularmente revisar e atualizar as configurações de sistemas e aplicativos para garantir que estejam alinhadas com as melhores práticas de segurança e para corrigir eventuais falhas de configuração.

Avaliação de Riscos

- Realizar avaliações de riscos periodicamente para identificar novas ameaças, vulnerabilidades e mudanças no ambiente que possam afetar a segurança da informação.

Auditorias de Conformidade

- Conduzir auditorias para garantir a conformidade com regulamentações e políticas internas. Isso inclui auditorias específicas, como PCI DSS (Padrão de Segurança de Dados para a Indústria de Cartões de Pagamento), se aplicável.

Treinamento e Conscientização

- Realizar treinamentos regulares para conscientizar os funcionários sobre práticas seguras e promover a cultura de segurança da informação.

Relatórios de Incidentes

- Estabelecer procedimentos claros para relatar e investigar incidentes de segurança. Isso permite uma resposta rápida e eficaz a qualquer violação de segurança.

Gestão de Incidentes

Lidar eficientemente com incidentes de segurança da informação é crucial para minimizar danos e proteger os ativos de uma organização.

Preparação

- **Equipe de Resposta a Incidentes (CSIRT):** Estabelecer uma equipe dedicada para responder a incidentes, incluindo especialistas em segurança da informação, pessoal técnico e representantes de comunicação.
- **Plano de Resposta a Incidentes:** Desenvolver e manter um plano detalhado que aborda procedimentos específicos a serem seguidos em caso de incidente, incluindo roles e responsabilidades.

Detecção e Notificação

- **Sistemas de Detecção:** Implementar ferramentas de detecção de intrusões e monitorar ativamente logs de sistemas para identificar atividades suspeitas.
- **Canais de Notificação:** Estabelecer canais de comunicação claros e eficientes para relatar incidentes, interna e externamente, se necessário.

Análise e Classificação

- **Investigação Inicial:** Realizar uma análise preliminar para avaliar a natureza e a extensão do incidente.
- **Classificação de Incidente:** Classificar o incidente de acordo com a gravidade, impacto e tipo, permitindo uma alocação adequada de recursos.

Contenção e Mitigação

- **Isolamento de Sistemas Afetados:** Tomar medidas para isolar os sistemas afetados, minimizando a propagação do incidente.
- **Mitigação de Danos:** Implementar medidas para limitar os danos causados pelo incidente, como desativar contas comprometidas ou aplicar patches de segurança.

Recuperação

- **Restauração de Sistemas:** Trabalhar na restauração dos sistemas afetados a partir de backups confiáveis.

- **Verificação de Integridade:** Certificar-se de que os sistemas restaurados estejam livres de malware e outras ameaças.

Comunicação

- **Comunicação Interna e Externa:** Informar as partes interessadas internas e externas, incluindo funcionários, clientes, parceiros e autoridades, conforme necessário.
- **Gerenciamento de Crises:** Designar porta-vozes e gerentes de crise para lidar com a comunicação externa e garantir uma mensagem coesa.

Investigação Pós-Incidente

- **Análise de Causa Raiz:** Conduzir uma investigação pós-incidência para identificar as causas raízes do incidente e prevenir recorrências.
- **Melhoria Contínua:** Utilizar as lições aprendidas para aprimorar políticas, procedimentos e controles de segurança.

Notificação de Autoridades e Reguladores

- **Conformidade Legal:** Cumprir com as obrigações legais e regulamentares em relação à notificação de incidentes de segurança.
- **Cooperação com Autoridades:** Colaborar com autoridades competentes, como órgãos reguladores e forças policiais, quando necessário.

Documentação e Relatório

- **Documentação Completa:** Manter registros detalhados de todas as etapas tomadas durante a resposta ao incidente.
- **Relatórios Pós-Incidente:** Preparar relatórios pós-incidência para análise interna e, se necessário, compartilhar informações com partes externas relevantes.

Treinamento e Exercícios Simulados

- **Treinamento Contínuo:** Realizar treinamentos regulares para a equipe de resposta a incidentes, bem como exercícios simulados para testar a eficácia do plano de resposta.

Backup e Recuperação

A elaboração de políticas para realizar backups regulares e garantir a recuperação de dados é uma parte crucial de qualquer política de segurança da informação. Essas políticas visam proteger os dados críticos da organização contra perda, corrupção ou danos.

Identificação de Dados Críticos

- Identificar os dados críticos para a operação da organização, incluindo informações sensíveis, bancos de dados, configurações de sistemas e outros ativos essenciais.

Frequência de Backup

- Estabelecer uma programação de backup regular com base nas necessidades da organização. Isso pode variar de acordo com a frequência de alterações nos dados, mas é comum realizar backups diários ou semanais.

Tipos de Backup

- Definir os tipos de backup a serem utilizados, como backups completos, incrementais ou diferenciais, dependendo dos requisitos de recuperação e eficiência de armazenamento.

Local de Armazenamento de Backups

- Determinar locais seguros e isolados para armazenar os backups. Isso pode incluir servidores dedicados, serviços de armazenamento em nuvem ou mídias offline.

Ciclo de Retenção

- Estabelecer uma política de ciclo de retenção para determinar por quanto tempo os backups serão mantidos. Isso deve levar em consideração requisitos regulatórios e a necessidade de recuperar versões mais antigas dos dados.

Testes de Recuperação

- Regularmente, testar os procedimentos de recuperação para garantir que os backups sejam eficazes e os dados possam ser restaurados com sucesso.

Monitoramento Automático

- Implementar sistemas de monitoramento automático para verificar regularmente a integridade dos backups e identificar possíveis problemas antes que afetem a recuperação.

Criptografia de Backups

- Utilizar criptografia para proteger os backups, tanto durante a transferência para o local de armazenamento quanto durante o armazenamento em si.

Autenticação e Controle de Acesso

- Restringir o acesso aos backups apenas a pessoal autorizado. Implementar autenticação robusta e controles de acesso para garantir a segurança dos dados armazenados.

Documentação e Catalogação

- Manter uma documentação detalhada dos procedimentos de backup, incluindo informações sobre o que está sendo backup, a frequência, os tipos de backup e os procedimentos de recuperação.

Backup de Configurações e Sistemas

- Além de dados, assegurar-se de incluir backups das configurações de sistemas, scripts e quaisquer elementos necessários para uma restauração completa e funcional.

Treinamento de Pessoal

- Fornecer treinamentos regulares para a equipe responsável pelos backups, garantindo que eles estejam cientes dos procedimentos e melhores práticas.

Notificação de Falhas

- Estabelecer procedimentos claros para notificar imediatamente a equipe de TI em caso de falha no backup, para que ações corretivas possam ser tomadas rapidamente.

Avaliação Contínua

- Avaliar continuamente a eficácia da política de backup e fazer ajustes conforme necessário, especialmente à medida que a infraestrutura de TI evolui.

Treinamento de Conscientização

Conscientizar os funcionários sobre segurança da informação é fundamental para criar uma cultura organizacional que valorize a proteção de dados e minimize os riscos de violações de segurança.

Treinamentos Regulares

- Realizar treinamentos periódicos para todos os funcionários, abordando questões de segurança da informação, boas práticas e os riscos associados a comportamentos inadequados.

Campanhas de Conscientização

- Desenvolver campanhas de conscientização com materiais visuais, e-mails informativos, cartazes e lembretes regulares para manter a segurança da informação em destaque na mente dos funcionários.

Simulações de Phishing

- Realizar simulações de phishing para testar a capacidade dos funcionários de identificar e relatar e-mails fraudulentos. Isso ajuda a reforçar a importância da vigilância online.

Políticas Claras e Acessíveis

- Desenvolver políticas claras de segurança da informação e torná-las facilmente acessíveis a todos os funcionários. Certificar-se de que compreendam as políticas e as consequências de violá-las.

Responsabilização

- Estabelecer uma cultura de responsabilização, incentivando os funcionários a assumirem a responsabilidade pela segurança dos dados e relatarem quaisquer atividades suspeitas.

Sensibilização para Dispositivos Móveis

- Educar os funcionários sobre práticas seguras no uso de dispositivos móveis, incluindo a necessidade de senhas, atualizações de segurança e o risco de se conectar a redes Wi-Fi públicas.

Workshops Interativos

- Realizar workshops interativos que envolvam os funcionários em cenários práticos relacionados à segurança da informação. Isso pode incluir simulações de incidentes e discussões em grupo.

Compartilhamento de Incidentes

- Promover a transparência ao compartilhar casos de incidentes de segurança da informação, destacando lições aprendidas e reforçando a importância de medidas preventivas.

Recursos Online e Intranet

- Disponibilizar recursos online e utilizar a intranet da empresa para fornecer informações atualizadas sobre segurança da informação, dicas práticas e respostas a perguntas frequentes.

Participação Executiva

- Envolver a liderança executiva na promoção da segurança da informação. A liderança ativa demonstra o comprometimento da alta administração com a proteção de dados.

Avaliação de Conhecimento

- Realizar avaliações periódicas para medir o nível de compreensão dos funcionários sobre práticas de segurança da informação. Usar os resultados para ajustar e aprimorar os programas de conscientização.

Comunicação Contínua

- Manter uma comunicação contínua sobre questões de segurança da informação por meio de canais internos, reuniões e outros meios de comunicação.

Conformidade Legal

Garantir que a política de segurança da informação esteja em conformidade com as leis e regulamentações aplicáveis é essencial para evitar penalidades legais, proteger a reputação da empresa e promover uma cultura de segurança robusta.

Conhecimento das Leis e Regulamentações

- Manter uma compreensão atualizada das leis e regulamentações relevantes ao setor e à localização geográfica da organização. Exemplos incluem GDPR na União Europeia, HIPAA nos EUA, LGPD no Brasil, entre outros.

Avaliação de Requisitos Específicos

- Identificar os requisitos específicos de segurança da informação estabelecidos por cada lei ou regulamento aplicável. Isso pode incluir medidas de proteção de dados, notificações de violações e requisitos de auditoria.

Análise de Riscos e Impacto

- Realizar uma análise de riscos para identificar como as políticas de segurança existentes podem se alinhar ou precisar ser ajustadas para atender aos requisitos legais. Avalie o impacto potencial de não conformidade.

Atualização de Políticas

- Atualizar as políticas de segurança da informação para incorporar os requisitos específicos de conformidade identificados. Certificar-se de que as políticas refletem as práticas e controles necessários.

Designação de Responsabilidades

- Atribuir responsabilidades claras para garantir a conformidade com as leis e regulamentações. Isso pode incluir um Encarregado de Dados (DPO) ou outra função específica de conformidade.

Treinamento e Conscientização

- Realizar treinamentos regulares para garantir que todos os funcionários estejam cientes dos requisitos legais, suas responsabilidades e as implicações da não conformidade.

Implementação de Controles Técnicos

- Implementar controles técnicos adequados para garantir a proteção dos dados, como criptografia, controle de acesso e monitoramento de atividades.

Registro e Documentação

- Manter registros detalhados das medidas tomadas para garantir a conformidade, incluindo auditorias internas, avaliações de riscos e ações corretivas implementadas.

Monitoramento Contínuo

- Implementar sistemas de monitoramento contínuo para garantir que as práticas de segurança estejam alinhadas com as leis e regulamentações em constante evolução.

Avaliação de Terceiros

- Se aplicável, avaliar a conformidade dos fornecedores e parceiros de negócios com as leis e regulamentações, garantindo que não haja riscos adicionais provenientes de terceiros.

Avaliação de Impacto da Proteção de Dados (DPIA)

- Realizar Avaliações de Impacto da Proteção de Dados sempre que necessário, especialmente em situações que envolvam o processamento de dados pessoais significativos e sensíveis.

Auditorias Internas e Externas

- Realizar auditorias internas e, se necessário, externas para avaliar a eficácia da conformidade com as leis e regulamentações. Usar os resultados para ajustar as práticas, conforme necessário.

Comunicação Transparente

- Manter uma comunicação transparente com as partes interessadas, incluindo clientes, fornecedores e autoridades regulatórias, sobre as medidas tomadas para garantir a conformidade.

Acompanhamento de Alterações Legislativas

- Manter-se informado sobre quaisquer alterações nas leis e regulamentações relevantes e ajustar as políticas de segurança da informação conforme necessário para permanecer em conformidade.

Abrangência, aprovação, divulgação e revisão

O conteúdo desta Política de Segurança da Informação aplica-se a todos os funcionários e prestadores de serviços relevantes da GestãoDS, no âmbito de suas atividades, atribuições e responsabilidades. Está aprovada pela Diretoria a qual está comprometida com a melhoria contínua do disposto neste normativo.

Está sendo publicada e comunicada para todos os funcionários, empresas contratadas de serviços de cibernética e clientes e partes externas relevantes, para o necessário cumprimento.

Um resumo da Política de Segurança da informação estará sendo divulgado ao público através do site da organização.

É obrigação de todo funcionário ou colaborador conhecer e praticar as disposições desta Política e assegurar que, quando necessário, prestadores de serviços sejam informados sobre as regras estabelecidas.

Será implementado um Programa de capacitação e de avaliação periódica de pessoal sobre as diretrizes desta Política.

Esta Política, juntamente com o Plano de Ação e respostas a incidentes será revisada anualmente ou quando mudanças significativas ocorrerem, assegurando a sua contínua pertinência, adequação e eficácia.

Revisão	Aprovação
Data	**Data**

Revisão	Aprovação
Data	**Data**

Revisão	Aprovação
Data	**Data**