TRUE - Tecnologia para a Vida
Proposição de Política de Segurança da Informação

Sumário

TRUE
Tecnologia para a vida

Justificativa

A política de segurança da informação é um documento fundamental para qualquer organização que lida com dados sensíveis ou informações críticas.

Ela estabelece diretrizes, princípios e procedimentos que visam proteger a confidencialidade, integridade e disponibilidade das informações da empresa, sob sua guarda ou responsabilidade, bem como para cumprir regulamentações e normas de segurança relevantes.

A justificativa para a implementação de uma política de segurança da informação é baseada em várias razões críticas:

Proteção dos ativos da organização

As informações são ativos valiosos para qualquer empresa, e sua perda, comprometimento ou destruição pode causar prejuízos significativos. A política de segurança da informação visa proteger esses ativos contra ameaças internas e externas.

Conformidade regulatória

Muitas organizações estão sujeitas a regulamentações governamentais e padrões da indústria que exigem a implementação de medidas de segurança da informação. A não conformidade pode resultar em multas substanciais e danos à reputação.

Proteção da privacidade

A política de segurança da informação ajuda a garantir a privacidade dos dados dos clientes, funcionários e parceiros de negócios. Isso é essencial para construir e manter a confiança das partes interessadas.

Prevenção de ataques cibernéticos

Com o aumento das ameaças cibernéticas, as organizações estão constantemente em risco de ataques, como malware, phishing e ransomware. A política de segurança da informação define medidas para prevenir, detectar e responder a esses ataques.

Redução de riscos e custos

Investir em segurança da informação pode ajudar a reduzir os riscos associados a incidentes de segurança, minimizando assim os custos relacionados à recuperação de dados perdidos, reparo de sistemas comprometidos e potenciais ações judiciais.

Continuidade dos negócios

A política de segurança da informação também inclui planos de continuidade de negócios que ajudam a garantir que a organização possa continuar suas operações, mesmo após incidentes de segurança, como desastres naturais ou ataques cibernéticos.

Fortalecimento da reputação (diferencial de mercado)

Uma organização que demonstra um compromisso sério com a segurança da informação pode melhorar sua reputação junto a clientes, parceiros e investidores, pois eles se sentirão mais confiantes na capacidade da empresa de proteger seus dados.

Boas práticas de governança

A política de segurança da informação é uma parte fundamental da governança corporativa. Ela demonstra que a empresa está comprometida em gerenciar seus ativos de informação de forma responsável e ética.

Em resumo, a implementação de uma política de segurança da informação é uma medida crítica para proteger os ativos da organização, garantir a conformidade com regulamentações, fortalecer a confiança das partes interessadas e reduzir riscos e custos associados a incidentes de segurança.

É uma parte essencial da gestão de riscos e da governança corporativa de qualquer empresa moderna.

Uma política de segurança da informação deve ser adaptada às necessidades específicas da organização e revisada periodicamente para garantir que permaneça eficaz e atualizada em relação às ameaças emergentes. Além disso, a adesão a essa política deve ser uma responsabilidade compartilhada por todos os membros da organização para garantir a proteção adequada das informações.

Objetivos

A política de segurança da informação tem como objetivo primordial proteger os ativos de informação da organização e os interesses de todas as partes envolvidas, ao mesmo tempo em que contribui para o cumprimento de regulamentações, a preservação da reputação e a garantia da continuidade dos negócios.

Ela define as metas gerais que a organização busca alcançar com suas práticas de segurança da informação e o motivo pelo qual essas práticas são fundamentais.

Confidencialidade

Proteger informações sensíveis e restritas contra acessos não autorizados, garantindo que apenas pessoas autorizadas tenham permissão para acessá-las.

Integridade

Manter a precisão, integridade e consistência dos dados, impedindo alterações não autorizadas, corrupção ou adulteração.

Disponibilidade

Garantir que as informações estejam disponíveis quando necessárias, minimizando interrupções ou tempos de inatividade não planejados.

Autenticidade

Assegurar que os usuários e sistemas sejam autenticados de maneira adequada para evitar falsificação de identidades.

Responsabilidade

Definir claramente as responsabilidades de todos os envolvidos na proteção das informações, desde os funcionários até a alta administração.

Conformidade legal

Cumprir as leis, regulamentações e normas relacionadas à segurança da informação, como LGPD, GDPR, HIPAA, ISO 27001, entre outras.

Resposta a incidentes

Estabelecer procedimentos para identificar, relatar e responder a incidentes de segurança da informação de maneira eficaz.

Proteger os ativos críticos

O propósito principal de uma política de segurança da informação é proteger os ativos de informação críticos da organização, como dados confidenciais, propriedade intelectual, informações financeiras e outros recursos de valor.

Minimizar riscos

Reduzir o risco de exposição a ameaças de segurança, como ataques cibernéticos, vazamentos de dados e perda de informações.

Preservar a reputação

Garantir que a organização mantenha sua reputação, evitando incidentes de segurança que possam prejudicar a confiança dos clientes, parceiros e partes interessadas.

Cumprir regulamentos

Cumprir as obrigações legais e regulatórias relacionadas à proteção de informações pessoais, confidenciais e sensíveis.

Promover a conscientização

Educar e capacitar os funcionários e demais partes interessadas sobre a importância da segurança da informação e seu papel na proteção dos ativos da organização.

Garantir a continuidade dos negócios

Manter a disponibilidade das informações e dos sistemas críticos, mesmo em situações adversas, para garantir a continuidade dos negócios.

Melhorar a eficiência operacional

Estabelecer procedimentos e práticas eficazes que, ao mesmo tempo, garantem a segurança e facilitam a eficiência operacional da organização.

Escopo

O escopo de uma política de segurança da informação define os limites e abrangência das diretrizes, princípios e procedimentos que serão aplicados para proteger os ativos de informação da organização.

É importante definir claramente o escopo para garantir que a política seja eficaz e relevante.

Ativos de informação

Identificar quais ativos de informação estão cobertos pela política: dados, sistemas, aplicativos, hardware, software, redes e qualquer outra coisa que seja relevante para a segurança da informação.

Pessoal

Determinar quais membros da organização e terceiros estão sujeitos à política: funcionários em todos os níveis, fornecedores, contratados e parceiros de negócios que tenham acesso a informações sensíveis.

Abrangência geográfica

Especificar onde a política de segurança da informação se aplica: locais físicos, como escritórios, data centers e filiais, bem como ambientes virtuais, como redes remotas ou de acesso móvel.

Tecnologias e sistemas

Indicar os sistemas de tecnologia da informação (TI) e infraestrutura de rede que estão sujeitos à política: servidores, dispositivos de rede, computadores pessoais e dispositivos móveis.

Tipos de informações

Definir os tipos de informações que estão protegidos pela política: informações financeiras, informações pessoais dos clientes, propriedade intelectual, dados de pesquisa e quaisquer outros dados críticos para o funcionamento da organização.

Ameaças e riscos

Identificar as ameaças e riscos específicos que a política visa abordar: ameaças cibernéticas, como malware e ataques de phishing), bem como riscos físicos, como incêndios, inundações e roubo de equipamentos.

Objetivos e metas

Especificar os objetivos de segurança da informação que a política busca alcançar: proteção da confidencialidade, integridade e disponibilidade dos dados, bem como a conformidade com regulamentações específicas.

Responsabilidades

Determine quem é responsável por implementar e manter a política de segurança da informação: alta administração, gerentes de TI, equipes de segurança da informação e funcionários individuais.

Conformidade e auditoria

Esclarecer como a conformidade com a política será monitorada e como as auditorias de segurança da informação serão conduzidas.

Comunicação e conscientização

Estabelecer diretrizes para a comunicação interna e conscientização sobre segurança da informação, incluindo capacitação e treinamento regular para funcionários e partes interessadas.

Revisão

Especificar como a política será revisada e atualizada ao longo do tempo para garantir que ela permaneça relevante e eficaz em face das mudanças no ambiente de ameaças e tecnológico.

O escopo da política de segurança da informação deve ser claro e abrangente o suficiente para cobrir todos os aspectos críticos da proteção de dados e ativos de informação da organização, mas também deve ser flexível o bastante para se adaptar a mudanças nas ameaças e nas necessidades da organização ao longo do tempo.

Responsabilidades

Uma política de segurança da informação define claramente as responsabilidades de diferentes partes dentro da organização para garantir a implementação eficaz das diretrizes de segurança.

As responsabilidades dentro de uma política de segurança da informação podem variar de acordo com o tamanho, complexidade e natureza da organização, mas é essencial que todas as partes envolvidas compreendam suas obrigações e contribuam para a proteção eficaz dos ativos de informação.

Alta Administração

- Definir uma cultura de segurança da informação na organização.
- Aprovar a política de segurança da informação e quaisquer revisões subsequentes.
- Alocar recursos financeiros e humanos para implementar medidas de segurança.
- Nomear um diretor de segurança da informação (ou equivalente) responsável pela gestão das políticas de segurança.

Diretor de Segurança da Informação (ou equivalente)

- Supervisionar e gerenciar todas as atividades de segurança da informação.
- Desenvolver, implementar e manter as políticas e procedimentos de segurança.
- Conduzir avaliações de riscos e garantir a conformidade com as normas de segurança.
- Reportar regularmente à alta administração sobre o estado da segurança da informação.

Funcionários e Usuários

- Conhecer e seguir as políticas de segurança da informação.
- Proteger informações confidenciais e ativos de informação.
- Relatar qualquer incidente de segurança ou comportamento suspeito.
- Participar de treinamentos de conscientização sobre segurança.

Gerentes e Supervisores

- Garantir que as equipes sob sua supervisão compreendam e sigam as políticas de segurança.
- Supervisionar o acesso a informações confidenciais.
- Tomar medidas disciplinares em caso de violação das políticas de segurança.

Equipe de TI

- Implementar e manter medidas de segurança técnica, como firewalls, antivírus e criptografia.
- Monitorar sistemas e redes em busca de atividades suspeitas.
- Responder a incidentes de segurança e realizar investigações forenses, se necessário.

Equipe de Recursos Humanos

- Desenvolver políticas de contratação e demissão que incluam verificações de antecedentes e treinamento em segurança da informação.
- Garantir que os funcionários tenham acesso apenas às informações necessárias para suas funções.

Equipe de Auditoria Interna

- Realizar auditorias de segurança para garantir a conformidade com as políticas.
- Identificar vulnerabilidades e recomendar melhorias.

Fornecedores e Terceiros

- Seguir as políticas de segurança da organização ao lidar com informações ou sistemas da empresa.
- Relatar qualquer incidente de segurança que envolva suas operações.

Comitê de Segurança da Informação

- Supervisionar a implementação das políticas de segurança.
- Tomar decisões sobre mudanças na política com base em avaliações de risco e ameaças emergentes.

Equipe de Comunicação

- Gerenciar a comunicação interna e externa em caso de incidentes de segurança.
- Manter os stakeholders informados sobre a política de segurança da informação.

Equipe de Treinamento e Conscientização

- Desenvolver programas de treinamento e conscientização em segurança da informação.
- Garantir que os funcionários estejam bem-informados e atualizados sobre as políticas de segurança.

Classificação de informações

A classificação de informações é um componente fundamental da política de segurança da informação (PSI).

Ela envolve a categorização de dados e informações em diferentes níveis de sensibilidade, para que medidas de segurança apropriadas possam ser aplicadas para protegê-las de acordo com seu valor e importância.

A classificação de informações ajuda a garantir que os recursos de segurança sejam alocados de forma eficaz e que as informações críticas sejam protegidas de acordo com suas necessidades.

É importante que uma organização defina suas próprias categorias de classificação de informações com base em suas necessidades e no contexto de suas operações. Além disso, a política de segurança da informação deve estabelecer diretrizes claras sobre como cada categoria de informação deve ser manuseada, armazenada, transmitida e descartada.

Isso geralmente envolve o uso de controles de acesso, criptografia, autenticação e outras medidas de segurança para proteger as informações de acordo com sua classificação.

A classificação de informações desempenha um papel fundamental na proteção dos ativos de informações de uma organização e na garantia de que medidas adequadas de segurança sejam implementadas para mitigar riscos de vazamento de dados e violações de segurança.

As categorias comumente usadas para classificar informações são:

Publico

Esta categoria inclui informações que são consideradas públicas e não confidenciais. Isso pode incluir informações que já foram divulgadas publicamente ou não têm valor estratégico para a organização.

Interno

Informações internas são aquelas que são destinadas apenas para uso interno na organização. Elas podem incluir documentos e comunicações que não devem ser compartilhados externamente, mas que também não são altamente confidenciais.

Confidencial

As informações confidenciais são aquelas com alto grau de sensibilidade e não devem ser acessadas ou compartilhadas por pessoas não autorizadas. Isso pode incluir dados financeiros, informações de clientes, estratégias de negócios e outros tipos de dados críticos para a organização.

Secreta

Informações secretas são as mais sensíveis e restritas. Elas são geralmente acessíveis apenas a um grupo muito limitado de pessoas com autorização de segurança especial. Isso pode incluir informações relacionadas à segurança nacional, propriedade intelectual altamente confidencial e outros dados extremamente sensíveis.

1. Acesso e autenticação

Em uma política de segurança da informação, as diretrizes relacionadas ao acesso e autenticação desempenham um papel crucial na proteção dos ativos de informação de uma organização.

Garantir que apenas pessoas autorizadas tenham acesso a informações sensíveis e sistemas é fundamental para evitar violações de segurança.

Uma política de segurança da informação bem elaborada relacionada ao acesso e autenticação ajuda a proteger as informações confidenciais e os sistemas críticos de uma organização, reduzindo o risco de violações de segurança e garantindo a conformidade com regulamentações de privacidade e segurança.

Essa política deve ser revisada e atualizada regularmente para se manter eficaz contra ameaças em constante evolução.

Controle de Acesso

- **Princípio do menor privilégio**

  Conceder a cada usuário ou sistema o menor nível de acesso necessário para realizar suas tarefas.

- **Controle de acesso baseado em função (RBAC)**

  Atribuir direitos de acesso com base nas funções e responsabilidades dos usuários dentro da organização.

- **Auditoria de acesso**

  Registrar e monitorar as atividades de acesso para detectar comportamentos suspeitos e rastrear ações de usuários.

Autenticação

- **Senhas seguras**

  Exija senhas fortes que incluam uma combinação de letras, números e caracteres especiais, e defina políticas de atualização regular de senhas.

- **Autenticação de dois fatores (2FA)**

  Incentivar ou exigir a autenticação de dois fatores para adicionar uma camada extra de segurança.

- **Biometria**

  Utilizar a autenticação biométrica, como impressão digital ou reconhecimento facial, quando apropriado para aumentar a segurança.

Gerenciamento de Identidade

- **Provisionamento e desativação de contas**

  Criar procedimentos para criar, modificar e desativar contas de usuário de forma rápida e eficaz quando necessário.

- **Revisões periódicas**

  Realizar revisões regulares das contas de usuário e seus níveis de acesso para garantir que estejam atualizados e apropriados.

Monitoramento e Detecção

- **Sistema de detecção de intrusões (IDS)**

  Implementar um IDS para identificar atividades suspeitas ou tentativas de acesso não autorizado.

- **Alertas de segurança**

  Configurar alertas para notificar a equipe de segurança sobre eventos de acesso não autorizado ou anormalidades.

Educação e Treinamento

- **Conscientização de segurança**

  Realizar treinamentos regulares para funcionários sobre boas práticas de segurança da informação, incluindo senhas seguras e como reconhecer ataques de phishing.

Políticas e Procedimentos

- **Política de senha**

  Estabelecer uma política clara para o uso de senhas e a frequência de alterações.

- **Política de bloqueio de contas**

  Definir procedimentos para bloquear contas após um número específico de tentativas de login malsucedidas.

Recuperação de Senha e Acesso de Emergência

- Criar procedimentos seguros para recuperação de senhas e acesso de emergência, mas com supervisão e controle rigorosos.

Acesso Remoto

- Implementar conexões VPN (Virtual Private Network) seguras para acessos remotos.
- Utilizar autenticação forte para acessos remotos, especialmente em redes públicas.

Política de Privacidade e Consentimento

- Respeitar as leis de privacidade e obtenha o consentimento adequado dos usuários para coletar, armazenar e processar seus dados pessoais.

2. Controle de acesso

Diretrizes para controlar quem pode acessar, modificar ou compartilhar informações confidenciais, incluindo a implementação de princípios de "necessidade de saber".

3. Monitoramento e auditoria

Procedimentos para monitorar o uso dos sistemas e dados, bem como auditorias regulares para garantir o cumprimento das políticas.

4. Proteção contra ameaças

Abordagem para proteger contra ameaças de segurança, incluindo vírus, malware, ataques cibernéticos e outras vulnerabilidades.

5. Gerenciamento de comunicação segura

Diretrizes para a comunicação segura de informações confidenciais, como o uso de criptografia e sistemas de mensagens seguras.

6. Gerenciamento de incidentes

Procedimentos para lidar com violações de segurança e incidentes, incluindo notificação de partes afetadas e autoridades reguladoras, quando necessário.

7. Treinamento e conscientização

Programas de treinamento e conscientização para funcionários, contratados e terceiros que lidam com informações sensíveis.

8. Conformidade legal e regulatória

Comprometimento com o cumprimento de regulamentos de segurança da informação, como GDPR, HIPAA, ISO 27001, entre outros.

9. Revisão e atualização

Procedimentos para revisar e atualizar a política de segurança da informação conforme necessário para se adaptar a novas ameaças e tecnologias.

10. Consequências por violações

Descrição das ações disciplinares e legais que serão tomadas em caso de violações da política.

11. Documentação

Registros e documentação que devem ser mantidos para comprovar a conformidade com a política.