**UNIVERSIDADE NOVE DE JULHO**

**UNINOVE**

**CURSO DE**

**CIÊNCIAS DA COMPUTAÇÃO**

**E**

**SISTEMAS DE INFORMAÇÃO**

**DISCIPLINA DE SEGURANÇA DA INFORMAÇÃO**

Professor Evandro Carlo Teruel

Integrantes do grupo:

DIEGO FERNANDES ARAUJO - 421100207

São Paulo - 2023

| **Controle de Versões** | | | |
| --- | --- | --- | --- |
| **Versão** | **Data** | **Autor** | **Notas da Revisão** |
|  |  |  |  |

Sumário

[1 Contexto geral](#_heading=h.gjdgxs) 3

[2 Objetivos deste documento (propósito)](#_heading=h.30j0zll) 3

[3 Adequação ao Propósito da Empresa](#_heading=h.1fob9te) 3

[4 Objetivos de Segurança da Informação](#_heading=h.3znysh7) 3

[5 Âmbito e Aplicação](#_heading=h.2et92p0) 3

[6 Responsabilidades e Funções](#_heading=h.tyjcwt) 3

[7 Classificação da Informação](#_heading=h.3dy6vkm) 5

[8 Acesso à Informação](#_heading=h.1t3h5sf) 5

[9 Gerenciamento de Senhas](#_heading=h.4d34og8) 7

[10 Gerenciamento de Dispositivos e Equipamentos](#_heading=h.2s8eyo1) 8

[11 Gestão de Ativos de Hardware e Software](#_heading=h.17dp8vu) 8

[12 Política de Backup e Recuperação](#_heading=h.3rdcrjn) 8

[13 Monitoramento e Detecção de Intrusões](#_heading=h.26in1rg) 8

[14 Conscientização e Treinamento](#_heading=h.lnxbz9) 8

[15 Política de Uso Aceitável](#_heading=h.35nkun2) 9

[16 Criptografia e Proteção de Dados](#_heading=h.1ksv4uv) 9

[17 Gestão de Incidentes de Segurança](#_heading=h.44sinio) 9

[18 Revisão e Atualização da Política](#_heading=h.2jxsxqh) 9

[19 Conformidade Legal e Regulatória](#_heading=h.z337ya) 9

[20 Comprometimento da Direção com Requisitos Aplicáveis](#_heading=h.3j2qqm3) 11

[21 Comprometimento da Direção com a Melhoria Contínua](#_heading=h.1y810tw) 12

[22 Disponibilidade da PSI para partes internas](#_heading=h.4i7ojhp) 12

[23 Disponibilidade da PSI para partes externas](#_heading=h.2xcytpi) 12

[24 Sanções e punições pelo não cumprimento da PSI](#_heading=h.1ci93xb) 12

# Contexto geral

Esta Política de Segurança da Informação (PSI) é um documento fundamental que estabelece a postura, diretrizes e compromissos da empresa em relação à segurança da informação. Ele atuará como um guia estratégico e define a postura da empresa em relação à segurança cibernética e à proteção de informações sensíveis, servindo como base para a tomada de decisões relacionadas à segurança e orienta as ações de todos os envolvidos na empresa.

# Objetivos deste documento (propósito)

A adequação da Política de Segurança da Informação (PSI) ao propósito da empresa é fundamental para garantir que a segurança da informação seja integrada de forma eficaz em todos os aspectos das operações da organização.

# Adequação ao Propósito da Empresa

A empresa está profundamente alinhada com os objetivos, valores e missão da empresa, e isso demonstra sua importância estratégica. A Microsoft é uma das maiores empresas de tecnologia do mundo, e a segurança da informação desempenha um papel crucial em todos os aspectos de suas operações.

# Objetivos de Segurança da Informação

A Microsoft como uma das maiores empresas de tecnologia do mundo, estabeleceu uma série de objetivos de segurança da informação específicos para garantir a proteção de seus ativos e a manutenção da confiança de seus clientes e parceiros.

# Âmbito e Aplicação

A Política de Segurança da Informação (PSI) da Microsoft abrange uma ampla gama de ativos de informação e envolve várias partes interessadas em suas operações.

# Responsabilidades e Funções

As responsabilidades e funções relacionadas à segurança da informação na Microsoft são claramente definidas e incluem uma variedade de equipes, gerentes e funcionários em toda a organização.

Alta Administração e Governança:

* Conselho de Administração: Define as diretrizes gerais e estratégias de segurança da informação, aprova políticas e aloca recursos.
* CEO (Chief Executive Officer): Estabelece a cultura de segurança, assume a responsabilidade final pela segurança da informação e fornece apoio executivo.
* CISO (Chief Information Security Officer): É o líder da equipe de segurança da informação, definindo a estratégia de segurança, monitorando riscos e comunicando-os à alta administração.

Equipe de Segurança da Informação:

* Gerente de Segurança da Informação: Responsável por supervisionar todas as atividades relacionadas à segurança da informação, incluindo políticas, procedimentos e controles de segurança.
* Analistas de Segurança: Monitoram continuamente ameaças e incidentes, respondem a incidentes de segurança, implementam controles e medidas de segurança e realizam auditorias internas.
* Arquiteto de Segurança: Projeta e implementa soluções de segurança, como firewalls, sistemas de detecção de intrusões e proteção contra malware.

Gerentes e Líderes de Equipe:

* Gerentes de Departamento: São responsáveis por implementar as políticas e práticas de segurança em suas equipes, garantindo que os funcionários sigam as diretrizes de segurança.

Funcionários:

* Todos os Funcionários: Têm a responsabilidade de seguir as políticas e práticas de segurança da informação da Microsoft, participar de treinamentos de segurança e relatar quaisquer incidentes ou preocupações.
* Usuários com Privilégios Especiais: Funcionários com acesso privilegiado a sistemas e informações críticas devem aderir a políticas rigorosas de segurança e realizar suas tarefas com responsabilidade.

Outras Funções Relacionadas:

* Equipe de Compliance e Auditoria: Garante que a Microsoft esteja em conformidade com regulamentações de segurança da informação, realiza auditorias internas e externas e gerencia programas de conformidade.
* Equipe de Desenvolvimento de Software: Integra práticas de segurança no ciclo de vida do desenvolvimento de software, garantindo que produtos e serviços sejam projetados com segurança.
* Equipe de Gerenciamento de Risco: Avalia riscos de segurança, realiza análises de impacto, desenvolve planos de mitigação e monitora riscos continuamente.
* Equipe de Resposta a Incidentes: Prepara-se para e responde a incidentes de segurança, minimizando o impacto e restaurando a normalidade após um incidente.
* Equipe de Conscientização em Segurança: Desenvolve e conduz programas de treinamento e conscientização em segurança para funcionários, contratantes e parceiros.
* Equipe de Gerenciamento de Acesso: Gerencia as políticas e práticas de controle de acesso, incluindo autenticação e autorização.

As responsabilidades e funções acima mencionadas trabalham em conjunto para garantir que a segurança da informação seja mantida em toda a Microsoft. A governança é fundamental, com a alta administração estabelecendo a direção estratégica e a equipe de segurança da informação implementando políticas e práticas para proteger ativos críticos de informação e garantir a conformidade regulatória. Todos os funcionários desempenham um papel na proteção da segurança da informação, contribuindo para uma cultura de segurança sólida em toda a organização.

# Classificação da Informação

A Microsoft, como muitas outras organizações, utiliza um sistema de classificação de informações para categorizar e proteger dados com base em sua sensibilidade e importância. Os níveis de classificação típicos incluem informações públicas, internas, confidenciais e secretas.

# Acesso à Informação

A Microsoft implementa diretrizes rigorosas para o acesso à informação, com o objetivo de garantir a segurança de seus ativos de informação. Essas diretrizes são fundamentais para proteger dados confidenciais, propriedade intelectual e informações sensíveis.

1. Princípio do Princípio do Princípio do Menor Privilégio (Least Privilege Principle): A Microsoft segue o princípio do menor privilégio, o que significa que os funcionários só têm acesso às informações e recursos que são estritamente necessários para realizar suas funções. Isso ajuda a minimizar o risco de acesso não autorizado.

2. Autenticação Multifatorial (MFA): A autenticação multifatorial é amplamente implementada para garantir que apenas usuários autorizados tenham acesso a sistemas e informações críticas. Isso requer que os usuários forneçam múltiplas formas de autenticação, como senha e um código de segurança temporário.

3. Controle de Acesso Baseado em Funções (Role-Based Access Control - RBAC): Os direitos de acesso são atribuídos com base nas funções e responsabilidades dos funcionários. Isso significa que diferentes níveis de acesso são concedidos de acordo com as necessidades específicas de trabalho de cada pessoa.

4. Políticas de Senha Forte: A Microsoft exige senhas fortes e de uso exclusivo, com períodos regulares de alteração de senha. Isso ajuda a evitar violações de segurança devido a senhas fracas ou comprometidas.

5. Auditoria e Monitoramento de Acesso: Todas as atividades de acesso são registradas e monitoradas. Isso permite a detecção precoce de atividades suspeitas e ações corretivas imediatas.

6. Revisões e Atualizações Regulares: Os direitos de acesso são revisados e atualizados regularmente. Isso garante que os funcionários ainda tenham acesso apenas às informações necessárias para suas funções.

7. Controle de Acesso a Locais Físicos: O acesso a instalações físicas, como data centers, é altamente restrito e controlado. Apenas pessoal autorizado pode entrar em áreas sensíveis.

8. Treinamento em Segurança: Os funcionários recebem treinamento regular em segurança da informação, incluindo a importância do acesso seguro e as melhores práticas para proteger informações.

9. Procedimentos de Encerramento de Acesso: Quando um funcionário deixa a organização ou muda de função, os procedimentos de encerramento de acesso são rigorosamente seguidos para garantir que o acesso seja revogado imediatamente.

10. Políticas de Segurança de Terceiros: Terceiros que acessem informações da Microsoft também são submetidos a políticas rigorosas de segurança e controles de acesso, incluindo fornecedores e parceiros.

Essas diretrizes de acesso à informação da Microsoft são parte integrante de sua abordagem abrangente de segurança da informação. Elas são projetadas para minimizar o risco de acesso não autorizado, proteger informações confidenciais e garantir que apenas as pessoas com as devidas autorizações tenham acesso aos ativos de informação da empresa.

# Gerenciamento de Senhas

A Microsoft adota políticas rigorosas para o gerenciamento de senhas, reconhecendo a importância das senhas fortes e do uso seguro para proteger seus ativos de informação.

Requisitos para Criação de Senhas:

Complexidade: As senhas devem ser complexas e incluir uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.

Comprimento Mínimo: As senhas devem ter um comprimento mínimo para aumentar sua segurança. Geralmente, um mínimo de 8 a 12 caracteres é recomendado.

Não uso de Informações Pessoais: As senhas não devem incluir informações pessoais facilmente identificáveis, como nomes próprios, datas de nascimento ou palavras relacionadas à empresa.

Uso Exclusivo: Cada senha deve ser exclusiva e não compartilhada com outras contas ou usuários.

Armazenamento Seguro de Senhas:

Não Armazenamento em Texto Plano: As senhas não devem ser armazenadas em texto plano em arquivos ou sistemas acessíveis.

Armazenamento Criptografado: As senhas devem ser armazenadas em formato criptografado para proteger contra vazamentos de dados.

Uso Seguro de Senhas:

Não Compartilhamento: As senhas não devem ser compartilhadas com colegas de trabalho ou outras pessoas, a menos que seja estritamente necessário para fins de trabalho.

Não Anotação em Locais Visíveis: As senhas não devem ser anotadas em áreas visíveis, como post-its colados em monitores.

Autenticação Multifatorial (MFA): Sempre que possível, a autenticação multifatorial deve ser ativada para adicionar uma camada extra de segurança.

Políticas de Alteração Regular de Senhas:

Redefinição Periódica de Senhas: As senhas devem ser redefinidas periodicamente, geralmente a cada 60 a 90 dias, para evitar que senhas comprometidas sejam usadas indefinidamente.

Histórico de Senhas: As senhas anteriores não podem ser reutilizadas em um determinado período de tempo (por exemplo, as últimas 6 senhas não podem ser reutilizadas).

Notificações de Alteração de Senhas: Os usuários devem ser notificados com antecedência sobre a necessidade de alterar suas senhas e receber lembretes regulares.

Diretrizes para Senhas Fortes:

Comprimento Adequado: As senhas devem ter pelo menos 8 a 12 caracteres de comprimento.

Complexidade: As senhas devem incluir uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.

Evitar Sequências Óbvias: Evitar sequências óbvias, como "123456" ou "password."

Não usar Palavras do Dicionário: Evitar o uso de palavras reais encontradas em dicionários.

Evitar Informações Pessoais: Não incluir informações pessoais, como nomes ou datas de nascimento.

Frase de Senha (Passphrase): Considerar o uso de frases de senha, que são mais longas e fáceis de lembrar, mas difíceis de adivinhar.

Essas políticas e diretrizes de gerenciamento de senhas da Microsoft são fundamentais para garantir senhas fortes e proteger contra acessos não autorizados. A empresa também incentiva os usuários a utilizar gerenciadores de senhas seguros para facilitar a criação e o armazenamento de senhas complexas e exclusivas para cada serviço ou conta.

# Gerenciamento de Dispositivos e Equipamentos

O gerenciamento de dispositivos e equipamentos é uma parte crítica da estratégia de segurança da informação da Microsoft. A empresa implementa diretrizes e procedimentos rigorosos para garantir que todos os dispositivos e equipamentos usados para processar, armazenar e transmitir informações estejam seguros.

# Gestão de Ativos de Hardware e Software

O gerenciamento adequado de ativos de hardware e software é essencial para a Microsoft para garantir a eficiência operacional, segurança e conformidade com regulamentações.

# Política de Backup e Recuperação

A Microsoft adota uma política abrangente de backup e recuperação para garantir a disponibilidade e a integridade de dados críticos. Essas diretrizes e procedimentos são essenciais para proteger informações valiosas e minimizar o impacto de perdas de dados

# Monitoramento e Detecção de Intrusões

A Microsoft adota uma abordagem rigorosa para o monitoramento e detecção de intrusões em suas redes, sistemas e aplicativos para garantir a segurança de suas operações.

# Conscientização e Treinamento

A Microsoft considera a conscientização e o treinamento em segurança da informação uma parte fundamental de sua estratégia de proteção de ativos de informação. A empresa se esforça para criar uma cultura de segurança onde todos os funcionários, contratados e outras partes interessadas estejam cientes das ameaças e riscos, saibam como se proteger e estejam comprometidos com a segurança dos ativos de informação.

# Política de Uso Aceitável

A Microsoft implementa uma política de uso aceitável para garantir que seus ativos de informação e recursos de TI sejam utilizados de maneira apropriada, segura e responsável. Essa política estabelece diretrizes e expectativas claras para funcionários, contratados, parceiros de negócios e outros usuários autorizados.

# Criptografia e Proteção de Dados

A Microsoft emprega diretrizes e procedimentos rigorosos relacionados ao uso de criptografia para proteger dados sensíveis e confidenciais, garantindo a integridade e a confidencialidade das informações, tanto em trânsito quanto em repouso. Essas práticas de criptografia são essenciais para manter a segurança da informação da empresa.

# Gestão de Incidentes de Segurança

A Microsoft implementa diretrizes e procedimentos rigorosos para a gestão de incidentes de segurança cibernética, garantindo a detecção, relato, avaliação e resposta eficaz a incidentes e violações de segurança. Essa abordagem é essencial para minimizar o impacto de incidentes e proteger os ativos de informação da empresa.

# Revisão e Atualização da Política

A revisão e atualização da política de segurança da informação são cruciais para garantir que ela permaneça eficaz e relevante ao longo do tempo, acompanhando as mudanças na tecnologia, ameaças cibernéticas e necessidades da empresa.

1. Comitê de Governança de Segurança:

Estabelecimento de um comitê de governança de segurança composto por partes interessadas-chave, incluindo representantes de TI, segurança da informação e liderança executiva.

2. Revisões Periódicas:

Realização de revisões periódicas da política de segurança da informação, com uma frequência definida, para avaliar a relevância e eficácia das diretrizes existentes.

3. Acompanhamento de Mudanças Regulatórias:

Monitoramento regular das mudanças em regulamentações de segurança e privacidade que possam afetar a política.

4. Avaliação de Ameaças Cibernéticas:

Avaliação contínua das ameaças cibernéticas emergentes e tendências de segurança para garantir que a política esteja alinhada com as melhores práticas de segurança.

5. Feedback dos Funcionários:

Solicitação de feedback dos funcionários e partes interessadas sobre a eficácia da política e áreas que podem precisar de ajustes.

6. Revisão das Melhores Práticas:

Acompanhamento das melhores práticas da indústria em segurança da informação e incorporação delas à política, quando apropriado.

7. Análise de Incidentes:

Análise de incidentes de segurança anteriores para identificar deficiências na política e áreas de melhoria.

8. Treinamento e Conscientização:

Atualização de programas de treinamento e conscientização para refletir as mudanças na política.

9. Processo de Mudança Controlada:

Implementação de um processo controlado para fazer alterações na política, incluindo aprovação da alta administração.

10. Comunicação de Alterações:

Comunicação eficaz de todas as alterações na política para garantir que os funcionários estejam cientes das atualizações.

11. Documentação de Revisões:

Documentação detalhada de todas as revisões da política, incluindo justificativas para as mudanças e datas de implementação.

12. Teste de Política Atualizada:

Realização de testes e simulações para garantir que a política atualizada seja eficaz na prática.

13. Auditorias e Avaliações Externas:

Realização de auditorias e avaliações externas periódicas para garantir a conformidade com regulamentações e padrões de segurança.

14. Manutenção de Registros:

Manutenção de registros detalhados de todas as versões anteriores da política para fins de auditoria e conformidade.

15. Ciclo de Revisão Definido:

Estabelecimento de um ciclo de revisão definido e um cronograma para garantir a revisão regular da política.

Ao seguir essas diretrizes, a Microsoft pode manter sua política de segurança da informação atualizada e adaptada às mudanças no ambiente de segurança cibernética e nas necessidades da empresa. Isso é fundamental para proteger continuamente os ativos de informação e manter a postura de segurança eficaz da organização.

# Conformidade Legal e Regulatória

A conformidade legal e regulatória é uma prioridade fundamental para a Microsoft, garantindo que a empresa cumpra todas as leis, regulamentos e normas relevantes relacionados à segurança da informação.

1. Identificação de Requisitos Regulatórios:

Identificação de todas as leis, regulamentos e normas relevantes que se aplicam à segurança da informação da Microsoft.

2. Avaliação de Impacto:

Avaliação do impacto desses requisitos regulatórios nas operações e práticas de segurança da informação da empresa.

3. Nomeação de Responsáveis pela Conformidade:

Designação de responsáveis pela conformidade regulatória que são encarregados de monitorar e garantir o cumprimento das obrigações legais.

4. Acompanhamento de Mudanças Regulatórias:

Monitoramento contínuo de mudanças em leis e regulamentos que possam afetar a segurança da informação.

5. Interpretação e Adaptação:

Interpretação das obrigações regulatórias para determinar como elas se aplicam à Microsoft e adaptação das políticas e práticas de segurança, conforme necessário.

6. Documentação de Conformidade:

Documentação detalhada de como a Microsoft está cumprindo cada requisito regulatório, incluindo registros e relatórios necessários.

7. Treinamento e Conscientização:

Treinamento regular dos funcionários e partes interessadas sobre os requisitos regulatórios relevantes e suas responsabilidades em relação à conformidade.

8. Auditoria Interna e Externa:

Realização de auditorias regulares, tanto internas quanto externas, para avaliar e verificar a conformidade com requisitos regulatórios.

9. Manutenção de Registros:

Manutenção de registros precisos e completos relacionados à conformidade, incluindo documentos de auditoria e relatórios de conformidade.

10. Comunicação com Autoridades Regulatórias:

Comunicação eficaz com autoridades regulatórias, incluindo relatórios de incidentes de segurança, quando necessário.

11. Avaliação de Riscos de Conformidade:

Avaliação contínua dos riscos de não conformidade e implementação de medidas para mitigá-los.

12. Conformidade Contratual:

Garantia de que os contratos com clientes e parceiros estejam alinhados com os requisitos regulatórios de segurança da informação

13. Atualização de Políticas e Procedimentos:

Atualização regular de políticas e procedimentos de segurança da informação para refletir as mudanças nos requisitos regulatórios

14. Cumprimento de Regulamentos de Proteção de Dados:

Estrita conformidade com regulamentos de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR), quando aplicável.

15. Revisão de Contratos de Fornecedores:

Revisão de contratos com fornecedores de serviços de terceiros para garantir que eles também cumpram os requisitos regulatórios.

O compromisso da Microsoft com a conformidade legal e regulatória é fundamental para proteger a privacidade e a segurança dos dados de seus clientes, garantindo ao mesmo tempo a integridade e a reputação da empresa.

# Comprometimento da Direção com Requisitos Aplicáveis

O comprometimento da alta direção com o cumprimento das leis, regulamentos e padrões relacionados à segurança da informação é um elemento essencial da cultura de segurança da Microsoft. A empresa reconhece a importância de liderar pelo exemplo e garantir que todos os níveis da organização estejam alinhados com os requisitos aplicáveis de segurança da informação.

# Comprometimento da Direção com a Melhoria Contínua

O comprometimento da alta direção com a melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI) e as práticas de segurança é essencial para manter a eficácia e a relevância da segurança da informação na Microsoft ao longo do tempo. A alta direção reconhece que a evolução das ameaças cibernéticas e das tecnologias exige um compromisso constante com aprimoramentos.

# Disponibilidade da PSI para partes internas

A disponibilidade da Política de Segurança da Informação (PSI) para partes internas da Microsoft é crucial para garantir que todos os colaboradores e partes interessadas tenham acesso às diretrizes e procedimentos de segurança da informação.

# Disponibilidade da PSI para partes externas

Compartilhar a Política de Segurança da Informação (PSI) com partes externas interessadas, como clientes, fornecedores e parceiros de negócios, é importante para demonstrar o compromisso da Microsoft com a segurança da informação e para garantir que todas as partes envolvidas estejam cientes das diretrizes de segurança.

# Sanções e punições pelo não cumprimento da PSI

As sanções e punições pelo não cumprimento da Política de Segurança da Informação (PSI) da Microsoft são essenciais para reforçar a importância da segurança da informação e garantir que todos os funcionários e equipes estejam comprometidos em seguir as diretrizes estabelecidas. As medidas disciplinares podem variar em gravidade, dependendo da natureza da violação e da política da organização

| **Aprovações** | | |
| --- | --- | --- |
| **Participante** | **Assinatura** | **Data** |
| Chief Executive Officer (CEO) | Erick Alves Santana | 12/09/2023 |
| Chief Security Officer (CSO) | Paulo Vinício Carreiro | 12/09/2023 |