**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** |
| 7 | 30/10 | Diego F. |  |

Sumário

[1 Contexto geral](#_gjdgxs) 3

[2 Objetivos deste documento (propósito)](#_30j0zll) 3

[3 Estabelecimento do contexto](#_1fob9te) 4

[3.1 Contexto Interno](#_3znysh7) 4

[3.2 Contexto externo](#_2et92p0) 5

[4 Identificação de risco](#_tyjcwt) 6

[5 Análise de riscos](#_3dy6vkm) 7

[6 Avaliação de riscos](#_1t3h5sf) 7

[7 Tratamento de riscos](#_4d34og8) 15

[8 Comunicação e consulta](#_2s8eyo1) 16

[9 Monitoramento e Análise Crítica](#_17dp8vu) 17

# Contexto geral

Um Programa de Gestão de Riscos de Segurança da Informação (PGRSI) baseado na norma ABNT NBR ISO/IEC 27005:2023 compreende a estrutura abrangente e contínua implementada por uma organização para identificar, avaliar, tratar e monitorar os riscos associados à segurança da informação. Esse programa engloba a definição de políticas, processos e procedimentos, bem como a alocação de recursos e a coordenação de esforços para garantir a proteção dos ativos de informação, a conformidade regulatória e a manutenção da resiliência contra ameaças internas e externas, por meio de abordagens de análise, mitigação e adaptação constantes.

# Objetivos deste documento (propósito)

O objetivo deste documento é estabelecer uma descrição clara do motivo pelo qual a Gestão de Riscos de Segurança da Informação (GRSI) está sendo implementada na Microsoft, bem como identificar os principais objetivos a serem alcançados com essa implementação.

Motivo para Implementação da GRSI na Microsoft:

A Microsoft reconhece a importância crítica da segurança da informação em um ambiente tecnológico em constante evolução e altamente conectado. Com a crescente quantidade de dados confidenciais e informações sensíveis que a empresa lida diariamente, a necessidade de uma abordagem estruturada e abrangente para gerenciar os riscos de segurança da informação tornou-se imperativa.

A implementação da Gestão de Riscos de Segurança da Informação (GRSI) é motivada pelos seguintes fatores:

Proteção de Ativos: A Microsoft possui ativos valiosos em termos de propriedade intelectual, informações confidenciais dos clientes e parceiros, dados de funcionários e outros recursos críticos. A GRSI visa proteger esses ativos contra ameaças internas e externas.

Cumprimento Regulatório: Como uma empresa global, a Microsoft está sujeita a diversas regulamentações de segurança da informação, como o Regulamento Geral de Proteção de Dados (GDPR) e leis de privacidade de dados em várias jurisdições. A implementação da GRSI ajuda a garantir o cumprimento dessas regulamentações.

Reputação da Marca: A Microsoft tem uma reputação a zelar. Uma violação de segurança da informação pode prejudicar gravemente a confiança dos clientes e a imagem da marca. A GRSI visa mitigar esse risco, garantindo que a empresa seja reconhecida como um líder em segurança.

Continuidade de Negócios: Interrupções causadas por incidentes de segurança da informação podem impactar negativamente a continuidade dos negócios. A GRSI busca identificar e mitigar riscos que poderiam interromper as operações da Microsoft.

Objetivos da Implementação da GRSI:

A implementação da Gestão de Riscos de Segurança da Informação na Microsoft tem como principais objetivos:

Identificação de Riscos: Identificar e avaliar os riscos de segurança da informação que a Microsoft enfrenta, levando em consideração ameaças internas e externas.

Mitigação de Riscos: Desenvolver estratégias e controles para mitigar os riscos identificados, incluindo medidas preventivas e corretivas.

Cumprimento Regulatório: Assegurar que as políticas e práticas de segurança da informação estejam em conformidade com as regulamentações relevantes, garantindo a proteção adequada dos dados.

Proteção de Ativos: Garantir a segurança de ativos críticos, incluindo informações confidenciais, sistemas de TI e infraestrutura de rede.

Treinamento e Conscientização: Educar os funcionários e partes interessadas sobre boas práticas de segurança da informação e garantir que todos compreendam suas responsabilidades na proteção dos dados.

Resposta a Incidentes: Desenvolver planos de resposta a incidentes para lidar eficazmente com violações de segurança da informação, minimizando o impacto e restaurando a normalidade rapidamente.

Melhoria Contínua: Estabelecer um ciclo de melhoria contínua para a GRSI, revisando e atualizando regularmente políticas, procedimentos e controles de segurança.

# Estabelecimento do contexto

## Contexto Interno

* + 1. Hierarquia Interna: Compreender a estrutura organizacional da Microsoft, identificando as áreas e departamentos relevantes para a GRSI, bem como as responsabilidades e autoridades de cada um.
    2. Documentos e Referências: Analisar políticas, diretrizes e documentos internos relacionados à segurança da informação, como manuais de segurança, políticas de acesso, e outras referências que orientam as práticas de segurança.
    3. Cultura Corporativa:Avaliar a cultura da empresa em relação à segurança da informação, incluindo o grau de conscientização e comprometimento dos funcionários com as práticas de segurança.
    4. Ativos e Infraestrutura: Identificar os ativos críticos da Microsoft, incluindo dados confidenciais, sistemas de TI, servidores, e redes, bem como sua localização e importância para a organização.
    5. Processos: Compreender os processos de negócios da Microsoft e como a segurança da informação está integrada a esses processos, identificando potenciais vulnerabilidades.
    6. Parceiros e Terceiros:Avaliar a relação da Microsoft com parceiros de negócios e terceiros que podem ter acesso a informações sensíveis ou afetar a segurança da empresa.
    7. Histórico Interno: Analisar incidentes de segurança passados, violações de dados ou problemas de segurança que ocorreram na Microsoft para aprender com as lições do passado.

## Contexto externo

* + 1. Leis e regulamentos: Conhecer as leis e regulamentos relevantes para a indústria e localizações em que a Microsoft opera, incluindo normas de proteção de dados, privacidade e requisitos de notificação de violações.
    2. Evolução de ameaças: Acompanhar as tendências em ameaças cibernéticas, como malware, phishing, engenharia social e ataques avançados, para estar preparado para novas ameaças.
    3. Mercado: Considerar as condições do mercado, incluindo mudanças nas demandas dos clientes, concorrência e tendências de tecnologia que possam impactar a segurança da informação.
    4. Novas tecnologias: Avaliar o impacto de novas tecnologias, como a computação em nuvem, Internet das Coisas (IoT) e inteligência artificial, na segurança da informação da Microsoft.
    5. Comunidade de Segurança: Participar ativamente da comunidade de segurança da informação, trocar informações e melhores práticas com outros profissionais da área.
    6. Política e Economia: Levar em consideração eventos políticos e econômicos globais que possam afetar a segurança da informação, como regulamentações comerciais e instabilidades econômicas.
    7. Parceiros e Concorrentes: Monitorar as práticas de segurança de parceiros de negócios e concorrentes para se manter atualizado e competitivo em termos de segurança da informação.

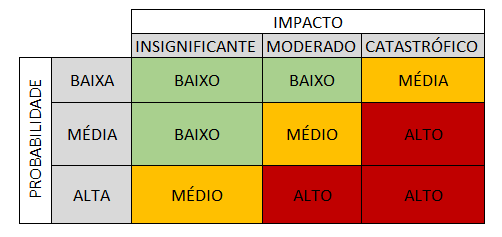
# Identificação de risco

Está tabela que ilustra alguns exemplos de riscos de segurança da informação e seus respectivos proprietários de acordo com a Norma ISO/IEC 27005:2023. Lembre-se de que essa é apenas uma representação ilustrativa e que na prática, a identificação de riscos pode ser mais detalhada e específica para a Microsoft.

| **Risco de segurança da informação** | **Proprietário do risco** |
| --- | --- |
| Ataque de malware | Equipe de segurança de TI |
| Acesso não autorizado a dados | Gerente de TI |
| Vazamento de informações Sensíveis | Gerente de privacidade de dados |
| Falha de hardware | Equipe de operações de TI |
| Desastre natural | Gerente de continuidade de negócios |
| Erro humano | RH |
| Concorrência desleal | Jurídico |
| Ataque de engenharia social | Equipe de segurança da informação |
| Falha de atualizações de segurança | Equipe de segurança de TI |

# Análise de riscos

Está matriz de riscos que ilustra a probabilidade, impacto e nível de cada risco de segurança da informação, com base nas informações fornecidas:



| **Risco de Segurança da informação** | **Probabilidade** | **Impacto** | **Nível de risco** |
| --- | --- | --- | --- |
| Ataque de malware | **Médio** | **Alto** | **Alto** |
| Acesso não autorizado a dados | **Baixo** | **Alto** | **Médio** |
| Vazamento de informação sensíveis | **Alto** | **Alto** | **Alto** |
| Falha de hardware | **Baixo** | **Médio** | **Baixo** |
| Desastre natural (ex: inundação) | **Baixo** | **Alto** | **Médio** |
| Erro humano | **Médio** | **Médio** | **Médio** |
| Concorrência desleal | **Baixo** | **Alto** | **Médio** |
| Ataque de engenharia social | **Alto** | **Médio** | **Alto** |
| Falta de atualização de segurança | **Médio** | **Médio** | **Alto** |

# Avaliação de riscos

A avaliação de riscos desempenha um papel fundamental no processo de gerenciamento de riscos da Microsoft, assim como em qualquer organização. Ela ajuda a Microsoft a tomar decisões informadas sobre como priorizar e abordar os riscos identificados. As considerações mencionadas na etapa de Avaliação de Riscos incluem:

| **Risco** | **Descrição do risco** | **Opção de tratamento de risco** | **Controles Necessários** | **Justificativa para a seleção da opção de tratamento de risco** |
| --- | --- | --- | --- | --- |
| Ataque de malware | Ameaça de software malicioso (malware) infecta sistemas de computador, dispositivos, redes ou aplicativos, causando danos, comprometendo a integridade dos dados e a privacidade das informações. | Implementação de Software de Segurança e Atualizações Regulares. | Antivírus e Antimalware  Firewalls  Política de Atualização  Conscientização do Usuário  Monitoramento  Contínuo  Backup de Dados | A implementação de software de segurança e atualizações regulares é a opção escolhida devido à sua eficácia comprovada na prevenção de ataques de malware.  Os malwares estão em constante evolução, tornando essencial manter sistemas e software atualizados para detectar e neutralizar as últimas ameaças. |
| Acesso não autorizado a dados | Possibilidade de indivíduos não autorizados ou não autenticados obterem acesso a informações confidenciais ou sensíveis, resultando em violações de privacidade, roubo de informações, potencial exposição a dados pessoais ou empresariais e perda de controle sobre os dados. | Implementação de Controles de Acesso e Autenticação Forte. | Políticas de Controle de Acesso  Autenticação Multifatorial (MFA)  Gerenciamento de Identidades  Auditoria de Acesso a Dados  Criptografia de Dados  Monitoramento Contínuo | A implementação de controles de acesso e autenticação forte é a opção escolhida devido à sua eficácia em reduzir o risco de acesso não autorizado a dados.  A MFA, em particular, é uma medida crucial para evitar que invasores obtenham acesso a sistemas ou dados confidenciais, mesmo que tenham obtido as credenciais de um usuário. |
| Vazamento de informação sensíveis | Ameaça de divulgação não autorizada de dados confidenciais, proprietários ou pessoais que podem resultar em sérias consequências, como perda de privacidade, danos à reputação, violação de regulamentações de privacidade, prejuízo financeiro e exposição a responsabilidades legais. | Implementação de Políticas de Classificação de Dados e Proteção de Dados. | Classificação de Dados  Controles de Acesso  Criptografia de Dados  Monitoramento de Atividades  Conscientização dos Funcionários  Políticas de Retenção de Dados | A implementação de políticas de classificação de dados e proteção de dados é uma escolha sólida para mitigar o risco de vazamento de informações sensíveis, pois aborda o problema de maneira abrangente.  A classificação de dados ajuda a identificar os ativos mais críticos, permitindo a aplicação de controles de segurança adequados, como restrições de acesso e criptografia. |
| Falha de hardware | Ameaça de mau funcionamento ou quebra de componentes de hardware em sistemas de computadores, servidores, dispositivos eletrônicos ou infraestrutura crítica de TI. | Implementação de Redundância de Hardware e Planos de Continuidade de Negócios. | Hardware Redundante  Balanceamento de Carga  Planos de Continuidade de Negócios (BCP)  Monitoramento Proativo  Manutenção Preventiva  Backup de Dados | A implementação de redundância de hardware e planos de continuidade de negócios é uma escolha apropriada para mitigar o risco de falha de hardware, pois aborda as consequências potencialmente graves dessas falhas.  A redundância de hardware permite que a operação continue mesmo quando um componente falha, garantindo a disponibilidade contínua de sistemas críticos. |
| Desastre natural (ex: inundação) | Ameaça de eventos catastróficos e imprevisíveis, como enchentes, terremotos, incêndios florestais, tempestades, entre outros, que podem causar danos significativos à infraestrutura, equipamentos, dados e operações de uma organização. | Elaboração de um Plano de Recuperação de Desastres (DRP) e a Implementação de Backup e Armazenamento Seguro de Dados. | Plano de Recuperação de Desastres (DRP)  Backup de Dados e Arquivamento  Testes e Treinamento  Local de Recuperação  Política de Seguro  Monitoramento de Alertas Meteorológicos | A elaboração de um Plano de Recuperação de Desastres e a implementação de backup e armazenamento seguro de dados são escolhas essenciais para mitigar o risco de desastres naturais, porque permitem que a organização se prepare para situações de emergência e minimize o impacto em suas operações. |
| Erro humano | Ameaça de ações ou decisões equivocadas de pessoas dentro de uma organização que podem resultar em incidentes, falhas, perdas financeiras, danos à reputação e violações de segurança. | Capacitação e Treinamento de Funcionários, juntamente com a Implementação de Controles de Segurança. | Treinamento de Conscientização em Segurança  Treinamento de Habilidades Específicas  Políticas e Procedimentos Documentados  Controles de Acesso  Revisões e Auditorias  Monitoramento de Comportamento | A capacitação e o treinamento de funcionários, juntamente com a implementação de controles de segurança, são essenciais para mitigar o risco de erro humano, pois abordam a raiz do problema.  A conscientização e a educação dos funcionários ajudam a reduzir os erros decorrentes da falta de conhecimento ou desatenção. |
| Concorrência desleal | Ameaça de ações antiéticas ou ilegais por parte de concorrentes ou terceiros que podem prejudicar a posição de mercado de uma empresa. | Monitorização Legal e Proteção de Propriedade Intelectual | Registro de Propriedade Intelectual  Assessoria Jurídica  Monitoramento da Concorrência  Compliance com a Lei  Educação e Conscientização  Medidas de Resposta Legal | A monitorização legal e a proteção de propriedade intelectual são essenciais para mitigar o risco de concorrência desleal, uma vez que as práticas desonestas muitas vezes envolvem violações de propriedade intelectual e questões legais.  O registo de propriedade intelectual oferece proteção legal sólida para os ativos da empresa, tornando mais difícil para os concorrentes explorarem esses ativos de forma injusta. |
| Ataque de engenharia social | Ameaça em que indivíduos mal-intencionados usam manipulação psicológica e técnicas de persuasão para enganar pessoas ou funcionários de uma organização a fim de obter informações confidenciais, acesso a sistemas, ou induzi-los a realizar ações prejudiciais. | Conscientização e Treinamento em Segurança | Treinamento em Conscientização de Segurança  Políticas e Procedimentos de Segurança  Verificação de Identidade  Avaliação de Riscos de Engenharia Social  Simulações de Ataques de Engenharia Social  Relatórios de Incidentes | A conscientização e o treinamento em segurança são cruciais para mitigar o risco de ataques de engenharia social, pois esses ataques exploram a vulnerabilidade humana.  Ao educar os funcionários sobre as táticas de engenharia social e promover uma cultura de segurança, a organização capacita seus membros a identificar e resistir a tentativas de manipulação. |
| Falta de atualização de segurança | Ameaça de exposição a vulnerabilidades de segurança em sistemas, aplicativos e dispositivos devido à não aplicação de patches de segurança ou atualizações de software. | Gestão de Ativos e Patch Management (Gerenciamento de Patches) | Inventário de Ativos  Avaliação de Vulnerabilidades  Política de Atualização  Testes de Patches  Implantação de Patches Automatizada  Monitoramento Contínuo | A gestão de ativos e o gerenciamento de patches são opções de tratamento de risco eficazes para combater a falta de atualização de segurança, uma vez que abordam diretamente a exposição a vulnerabilidades conhecidas.  A identificação de ativos e avaliação de vulnerabilidades ajudam a identificar onde os patches são necessários, enquanto a política de atualização e a implantação automatizada garantem que as atualizações sejam aplicadas de forma consistente e oportuna. |

# Tratamento de riscos

O tratamento de riscos, como mencionado na sua descrição, é uma etapa crítica no processo de gerenciamento de riscos da Microsoft e de qualquer organização. Envolve a implementação de medidas para reduzir a probabilidade e o impacto dos riscos, garantindo que os níveis de risco estejam dentro dos limites aceitáveis da organização. Aqui estão alguns pontos importantes a serem considerados na etapa de Tratamento de Riscos:

**Abordagens Específica**s: É essencial identificar abordagens específicas para tratar cada risco identificado. Isso pode incluir a escolha de medidas como evitar, transferir, mitigar ou aceitar o risco, dependendo da natureza e da gravidade do risco.

**Medidas de Redução de Probabilidade e Impacto**: Indicar as medidas que serão implementadas para reduzir a probabilidade de ocorrência de riscos ou minimizar seus impactos. Isso pode envolver a implementação de controles de segurança, políticas, procedimentos, treinamento e outras ações relevantes.

**Riscos que Podem ser Evitados**: Identificar os riscos que podem ser evitados por meio de mudanças nas operações, processos ou atividades da organização. Isso pode incluir ajustes nas práticas comerciais para eliminar certos riscos.

**Riscos Transferíveis**: Identificar os riscos que podem ser transferidos para terceiros, como seguradoras ou provedores de serviços especializados. Isso envolve a compra de seguros ou a terceirização de certas atividades para reduzir a exposição ao risco.

**Riscos Aceitáveis**: Indicar quais riscos podem ser aceitos, seja porque o custo de tratamento é maior do que o possível impacto ou porque o risco é considerado aceitável dentro dos limites definidos pela organização.

**Responsabilidades e Controles**: Especificar claramente quem será responsável pela implementação das medidas de tratamento e pela gestão contínua dos riscos. Também é importante definir os controles de segurança específicos que serão utilizados para lidar com os riscos, abrangendo aspectos técnicos, organizacionais e legais.

**Monitoramento Contínuo**: Estabelecer mecanismos de monitoramento contínuo para avaliar a eficácia das medidas de tratamento e tomar ações corretivas quando necessário. Isso garante que as medidas permaneçam eficazes ao longo do tempo.

**Custos e Benefícios**: Avaliar os custos envolvidos na implementação das medidas de tratamento em relação aos benefícios esperados na redução de riscos. Isso ajuda a tomar decisões informadas sobre a alocação de recursos.

**Integração com Processos de Negócios**: Garantir que as medidas de tratamento sejam integradas de forma eficiente aos processos de negócios da Microsoft, para que sejam aplicadas de maneira consistente e eficaz em toda a organização.

# Comunicação e consulta

O gerenciamento e a minimização de riscos na organização começam com a compreensão dos tipos de riscos encontrados no local de trabalho moderno. Alguns riscos são impulsionados por eventos externos e fatores que estão fora do controle direto. Outros riscos são impulsionados por eventos internos e ações do usuário que podem ser minimizadas ou evitadas. Alguns exemplos são riscos de comportamentos e ações ilegais, inadequadas, não autorizadas ou antiéticas dos usuários em sua organização. Esses comportamentos incluem uma ampla gama de riscos internos dos usuários:

* Vazamentos de dados confidenciais e análise de dados
* Violações de confidencialidade
* Direitos de Propriedade Intelectual (IP)
* Fraude
* Informações privilegiadas
* Soluções de conformidade regulamentar

Os usuários no local de trabalho moderno têm acesso para criar, gerenciar e compartilhar dados em um amplo espectro de plataformas e serviços. Na maioria dos casos, as organizações têm recursos e ferramentas limitados para identificar e mitigar riscos em toda a organização e, ao mesmo tempo, atender aos padrões de privacidade do usuário.

O gerenciamento de risco interno usa a amplitude total do serviço e dos indicadores de terceiros para ajudá-lo a identificar, triagem e agir rapidamente sobre a atividade de risco. Ao usar logs do Microsoft 365 e do Microsoft Graph, o gerenciamento de risco interno permite que você defina políticas específicas para identificar indicadores de risco. Essas políticas permitem identificar atividades arriscadas e agir para mitigar esses riscos.

O gerenciamento de risco interno é centrado em torno dos seguintes princípios:

* Transparência: balancei a privacidade do usuário versus o risco da organização com a arquitetura de privacidade por design.
* Configurável: políticas configuráveis com base em grupos empresariais, geográficos e industriais.
* Integrado: fluxo de trabalho integrado entre soluções do Microsoft Purview.
* Acionável: fornece insights para habilitar notificações de revisor, investigações de dados e investigações de usuário.

Os alertas para identificação do problema são gerados automaticamente por indicadores de risco que correspondem às condições da política e são [exibidos no dashboard alertas](https://learn.microsoft.com/pt-br/purview/insider-risk-management-activities#alert-dashboard). Esse painel permite uma exibição rápida de todos os alertas que precisam de revisão, alertas abertos ao longo do tempo e estatísticas de alerta para a sua organização. Todos os alertas de política são exibidos com as seguintes informações para ajudá-lo a identificar rapidamente o status de alertas existentes e novos alertas que precisam de ação:

* ID
* Usuários
* Alerta
* Status
* Gravidade do alerta
* Tempo detectado
* Caso
* Status de caso
* Fatores de risco

# Monitoramento e Análise Crítica

Todos os sistemas comerciais que contêm dados confidenciais devem implementar uma estrutura de segurança. A complexidade do mecanismo de segurança geralmente é uma função da confidencialidade dos dados. Em um sistema que exija que os usuários sejam autenticados, você deve registrar:

* Todas as tentativas de entrada, quer elas falhem ou tenham êxito.
* Todas as operações executadas por – e os detalhes de todos os recursos acessados por – um usuário autenticado.
* Quando um usuário encerra uma sessão e sai.

O monitoramento pode ajudar a detectar ataques ao sistema. Por exemplo, um grande número de tentativas de logon com falha pode indicar um ataque de força bruta. Um aumento inesperado de solicitações pode ser o resultado de um ataque DDoS (de negação de serviço distribuído). Você deve estar preparado para monitorar todas as solicitações para todos os recursos, independentemente da origem dessas solicitações. Um sistema que tenha uma vulnerabilidade de logon pode expor acidentalmente recursos para o mundo exterior sem exigir que um usuário realmente entre.

Um recurso do monitoramento de segurança é a variedade de fontes das quais os dados surgem. Os diferentes formatos e níveis de detalhe geralmente exigem uma análise complexa dos dados capturados, para uni-los em um thread de informações coerente. Além dos casos mais simples (por exemplo, a detecção de um grande número de logons com falha ou tentativas repetidas de acesso não autorizado a recursos críticos), pode não ser possível executar processamentos complexos automatizados dos dados de segurança. Em vez disso, talvez seja preferível gravar esses dados, com carimbo de data/hora, mas na forma original, em um repositório seguro para permitir a análise manual por especialistas.

| **Aprovações** | | |
| --- | --- | --- |
| **Participante** | **Assinatura** | **Data** |
| Chief Executive Officer (CEO) | Erick Alves Santana | 19/09/2023 |
| Chief Security Officer (CSO) | Paulo Vinício Carreiro | 19/09/2023 |