| **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) infectar 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. |