O risco é inerente a atividade humana, sempre o acompanhando durante o passar do tempo. Cada atividade realizada acolhe um tipo de risco, sendo necessário assim dimensionar a solução ou alternativa que possa evitar a ocorrência do risco.

A definição de risco estabelecida pela norma ISO 31000 é “efeito da incerteza nos objetivos”. Em tudo o que fazemos causamos efeitos colaterais, a essa causa chamamos efeito “ação e reação”, quando estamos criando uma análise de risco, devemos antecipar todos os riscos que poderemos passar.

Bancos de Dados desprotegidos, usuário com acesso a informações privilegiadas sem permissão, computadores desprotegidos de supervisão, senhas fáceis de serem descobertas são exemplos de riscos que um sistema informatizado pode ocorrer.

No sistema SIG, usamos uma escala de 3 níveis para descrever cada risco, são elas “Alto risco”, “Médio risco”, “Baixo Risco”.

Alto Risco, são rupturas ou vazamento de informações que podem prejudicar financeiramente a organização que utiliza o software. Por exemplo acesso por terceiro a dados de contas bancárias ou a senha dos profissionais envolvidos, perca dos dados.

Médio risco, são erros e informações que podem levar o usuário a não conseguir utilizar o software ou até utiliza-lo de forma indevida, por exemplo, permitir deletar informações que não são do usuário. Cálculos indevidos, páginas com erros e links sem páginas.

Baixo Risco, ações que impeçam o usuário de utilizar o sistema, mas que não gerem dados indevidos ou que atrasem a utilização do sistema pelo usuário. Exemplo usuário não consegue se autenticar, botões sem ações, impossibilidade de acesso a determinada página mesmo com permissão.

|  |  |  |
| --- | --- | --- |
| **Nivel** | **Risco** | **Alternativa** |
| Baixo | Usuário esqueceu a senha | Cria uma opção para alterar a senha de acordo com algumas opções |
| Baixo | Senhas fáceis de lembrar | Criar mecanismo de complexidade de senhas |
| Baixo | Sem acesso ao sistema devido a quedas de rede | Criar um sistema offline com sincronização automático |
| Baixo | Acesso por outras pessoas do sistema a dados de outras pessoas | Criar sistema de níveis e permissões |
| Baixo | Falta de conhecimento do utilizador | Criar treinamentos onlines e presenciais para os utilizadores |
| Baixo | Hardware não compatíveis com as exigências mínimas | Indicar ao responsáveis pela infra-estrutura qual o equipamento mais adequado para ser utilizado e/ou quais serviços devem ser adquiridos |
| Médio | Link para páginas que não existem no sistema | Guardar todas as páginas que voltarem com erro 404 e informa-las ao administrador |
| Médio | Cálculo de Valores calculados de forma errada | Criar testes padronizados para cálculos e implementar opções de refazer cálculos e estorno |
| Médio | Páginas com erros de processamento | Criar log de páginas com erro 500 e informa-las ao administrador |
| Médio | Possibilidade de deletar informações que não sejam de propriedade do usuário | Criar sistema de voltar dados e guardar log de ações por usuários |
| Alto | Perca de dados | Mecanismo de backups diários com dois banco de dados distintos em sincronia |
| Alto | Acesso de dados por terceiros | Criptografia de dados com acesso apenas pelo sistema |
| Alto | Total perca dos dados | Criar backup fisicamente em mídia. |
| Alto | Servidores com falhas | Possibilidade de utilização de mais de um servidor |
| Alto | Queda de energia para alimentação dos servidores | Criação de um servidor na nuvem espelho para atender os clientes externos e uso de nobreaks |