1. Objetivo

Definir uma metodologia de identificação, avaliação e tratamento de riscos da informação na organização. A avaliação de riscos aplica-se a todo o Sistema de Gestão da Segurança da informação (SGSI), isto é, a todos os ativos de informações que são usados na organização ou que podem ter um impacto sobre a segurança da informação da organização.

1. Definições

**Ativo -** qualquer coisa que tenha valor para a organização.

Pode-se dizer que é tudo aquilo que por si só é importante (informação) ou cujo seu papel pode afetar a segurança da informação (preservação da confidencialidade, integridade e disponibilidade).

**Segurança da informação -** preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

**Confidencialidade -** propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

**Integridade -** propriedade de salvaguarda da totalidade e exatidão dos ativos.

**Disponibilidade -** propriedade de estar acessível e utilizável a pedido de uma entidade autorizada.

**Ameaça** – causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

**Vulnerabilidade** – fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

**Evento de segurança da informação -** uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controlos, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

**Incidente de segurança da informação -** um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

**Sistema de gestão da segurança da informação (SGSI) -** a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Nota: O sistema de gestão inclui estrutura organizacional, políticas, atividades de planeamento, responsabilidades, práticas, procedimentos, processos e recursos.

**Risco residual -** risco remanescente após o tratamento de riscos.

**Aceitação do risco -** decisão de aceitar um risco.

**Análise de riscos -** uso sistemático de informações para identificar fontes e estimar o risco.

**Análise/avaliação de riscos -** processo completo de análise e avaliação de riscos.

**Avaliação de riscos -** processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

**Gestão de riscos -** atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.

Nota: *A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos*.

**Tratamento do risco -** processo de seleção e implementação de medidas para modificar um risco.

**Declaração de aplicabilidade -** declaração documentada que descreve os objetivos de controlo e controles que são pertinentes e aplicáveis ao SGSI da organização.

Nota: Os objetivos de controlo e controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação.

1. Procedimento

A definição de uma boa metodologia de gestão de risco tem que contribuir para:

* A identificação de riscos;
* A análise/avaliação de riscos em termos das suas consequências para o negócio e da probabilidade da sua ocorrência;
* Que a probabilidade e a consequência dos riscos sejam comunicadas e entendidas;
* O estabelecimento de prioridades no tratamento de riscos;
* Que seja dada prioridade a ações que reduzam a ocorrência de riscos;
* Que todos os interessados sejam envolvidos nas decisões de gestão de risco e estejam informados do estado da gestão dos mesmos;
* A monitorização de eficácia do tratamento de risco;
* A revisão e monitorização periódicas dos riscos e do processo de gestão dos mesmos;
* A captura de informação que permita melhorar a abordagem de gestão de risco;
* A sensibilização de gestores e colaboradores para os riscos e as ações tomadas no sentido de os mitigar.

Os riscos devem ser geridos de acordo com o processo ilustrado na figura.



3.1. Análise e Avaliação dos Riscos

A análise e avaliação dos riscos é coordenada pelo CISO (Chief Information Security Officer) e por um elemento do Comité da Segurança da Informação, sendo utilizada para tal a Tabela de Avaliação de Riscos.

3.2. Identificação dos Ativos

A primeira etapa da avaliação de riscos é a identificação de todos os ativos de informação, isto é, de todos os ativos que podem afetar a confidencialidade, integridade e disponibilidade das informações na organização. Os ativos podem incluir documentos em papel ou formato eletrónico, aplicativos e bases de dados, pessoas, equipamentos de informação e comunicação, serviços internos e externos. Ao identificar os ativos, também é preciso identificar os seus "proprietários", as pessoas ou a unidade organizacional responsável para cada ativo, diferenciando-os por categorias de ativos.

3.3. Identificação dos Riscos

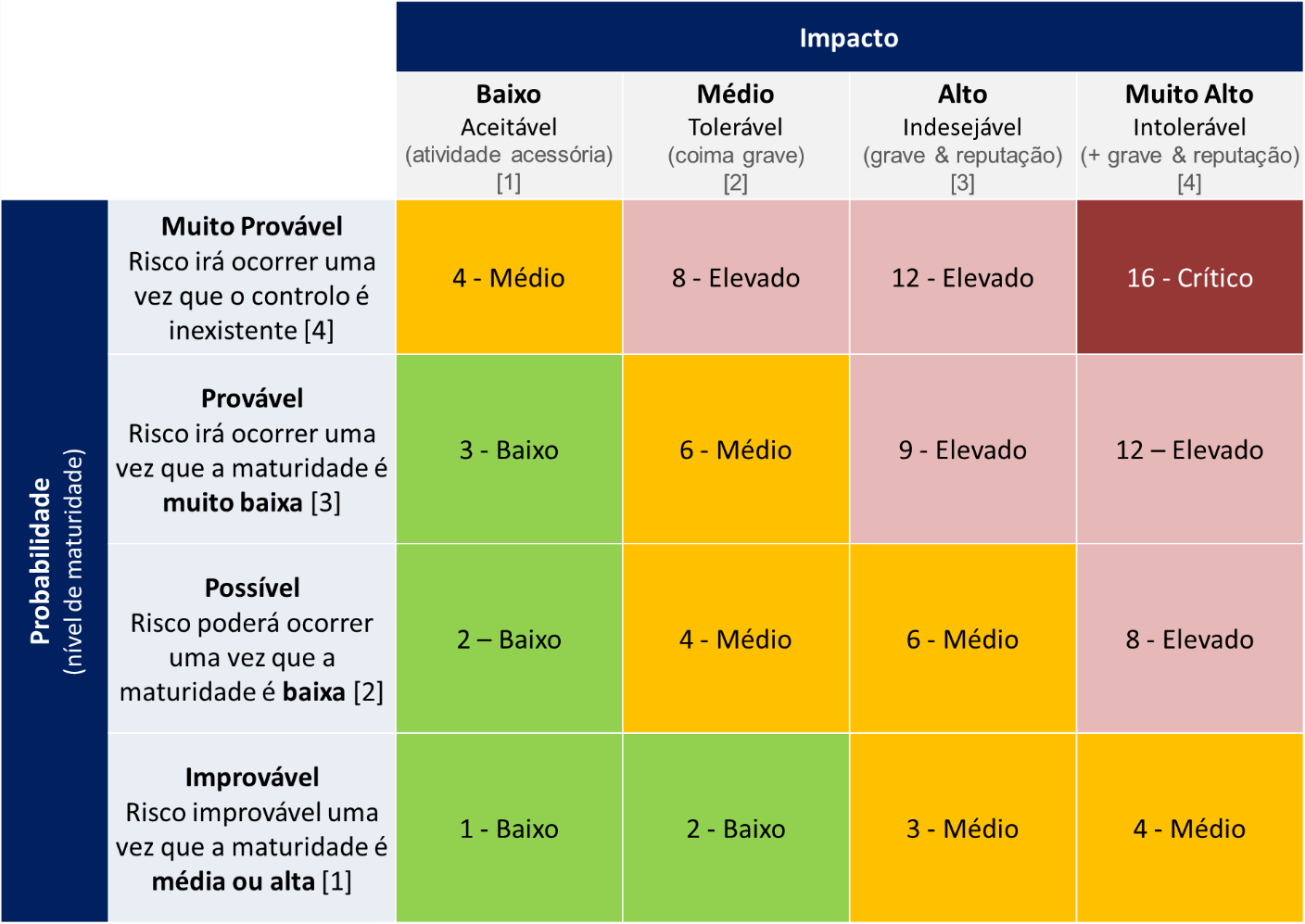
Na identificação dos riscos deve, ter-se em conta as ameaças, vulnerabilidades e consequências associadas a cada ativo.

Deve-se ter o cuidado de avaliar que cada ativo pode estar associado a diversas ameaças e cada ameaça pode estar associada a diversas vulnerabilidades.

3.4. Estimativa dos Riscos

Nesta fase, deve proceder-se à estimativa dos riscos que afetam a atividade da organização, avaliando-se para cada Risco, a Probabilidade e o Impacto:

O grau de impacto determinado deverá ter em consideração, as potenciais consequências da perda de confidencialidade, integridade e/ou disponibilidade do ativo e os controlos que já se encontram implementados e que possam contribuir para a redução do mesmo.



Os controlos de segurança existentes devem ser inseridos na coluna da Tabela de avaliação de riscos.

**Nível de Risco Final = Probabilidade \* Impacto**

3.5. Avaliação dos Riscos

Após se ter uma lista de todos os riscos estimados que ameaçam os ativos da organização, é necessário compará-los com os critérios previamente definidos para:

* Avaliação de risco: Que definem as várias categorias de riscos que se pretendem diferenciar e podem ser utilizadas para definir prioridades de tratamento dos mesmos;
* Aceitação de risco: Que definem as circunstâncias em que um determinado risco é considerado suficientemente negligenciável para não requerer qualquer tipo de tratamento.

Assim, é possível tomar decisões sobre ações a tomar, nomeadamente sobre quais os riscos que requerem ação e respetivas prioridades.

Contudo, nesta fase é também especialmente importante avaliar se há ou não confiança nos critérios definidos e na estimativa de riscos efetuada, principalmente durante as primeiras aplicações da metodologia. Caso haja dúvidas sobre a sua eficácia/adequação, devem efetuar-se os ajustes necessários e repetir a sua aplicação.

Assim, no final desta fase surge uma lista de riscos priorizada de acordo com os critérios adotados.

|  |  |  |
| --- | --- | --- |
| **Categoria** | **Nível de Risco** | **Descrição** |
| Crítico | 16 | São inaceitáveis, devem ter um tratamento prioritário imediato |
| Elevado | [8-12] | São inaceitáveis, devem ter um tratamento prioritário. |
| Médio | [4-6] | Poderão ser aceitáveis mediante formalização por parte da Administração. Caso contrário, requerem a existência de um plano de tratamento. |
| Baixo | ≤3 | São considerados aceitáveis, carecendo apenas de registo e não requerendo ações específicas de tratamento. |

3.6. Tratamento dos Riscos

Agora é necessário decidir o que fazer em relação a cada um deles, levando em consideração:

* A prioridade de cada um dos riscos;
* As opções de tratamento possíveis;
* Os benefícios esperados de cada uma das opções de tratamento existentes;
* O custo da implementação das opções de tratamento existentes, sendo que:
  + Se deve efetuar um esforço para reduzir o mais possível as consequências adversas dos riscos existentes;
  + Quando grandes reduções de risco podem ser conseguidas a um custo reduzido, essas opções devem ser implementadas;
  + Devem ser considerados riscos que, embora raros, possam ter consequências graves, e que justifiquem a adoção de tratamentos que não seriam justificáveis por critérios meramente económicos (por exemplo, a existência da controlos de continuidade de negócio);
  + Deve haver uma reflexão documentada sobre a não implementação de opções cujo custo seja considerado excessivo quando comparado com os benefícios esperados;



Processo de Tratamento de Risco

O resultado deverá ser formalizado num “Plano de Tratamento do Risco”. Após a definição do referido plano, determina-se os níveis residuais de risco, o que envolve uma atualização da apreciação de risco, considerando os efeitos dos vários tratamentos previstos. Caso o nível de risco residual ainda seja superior ao nível considerado aceitável, dever-se-á proceder a uma nova iteração do processo de tratamento de risco antes de se poder efetuar a aceitação.

### Redução do Risco

Esta opção de tratamento passa pela adoção de uma seleção de controlos que permitam obter níveis de risco residual considerados aceitáveis.

### Nota: No caso da opção pela Redução do Risco - seleção de controlos de segurança, é necessário avaliar o novo valor do impacto e a probabilidade na Tabela de tratamento de riscos, que resultará em um novo valor de risco após a implementação dos controlos.

### Retenção do Risco

Esta opção corresponde à decisão de aceitar um determinado risco, não tomando qualquer medida no sentido de o reduzir. Esta opção deve ser utilizada, caso o respetivo risco se encontre dentro dos critérios de aceitação definidos pela organização ou em situações em que não há nenhuma ação que possa evitar, reduzir ou transferir o risco (por exemplo, risco de alterações legislativas que impactem negativamente o negócio).

Para além disso, as consequências (legais, financeiras, etc.) de uma decisão deste tipo deverão ser cuidadosamente avaliadas, carecendo da aprovação da Gerência.

### Evitar o Risco

Quando um risco ou o custo da implementação do respetivo controlo é demasiadamente elevado, pode equacionar-se, descontinuar uma determinada atividade do negócio (p.e. deixando de comercializar um produto cuja qualidade não se consegue controlar), ou alterar as condições em que a mesma é levada a cabo (p.e. retirando ativos de locais propícios a furto, etc.).

### Partilha do Risco

Partilha do risco com terceiros mais capazes de o gerir de forma eficaz. Um exemplo deste tipo de tratamento será a subscrição de um seguro que cubra as consequências previstas ou a contratação de um prestador de serviços em quem delegar determinado tipo de atividades. Contudo, dado que daí podem advir novos riscos (franquias de prémios de seguro, risco de falha do prestador de serviços, etc..) ou a alteração de riscos já identificados, poderão ser necessárias medidas adicionais de tratamento de risco. Para além disso, a utilização deste tipo de opção carece de uma análise de risco ao parceiro envolvido.

## 3.7. Frequência da avaliação e do tratamento de riscos

A avaliação deve ser realizada pelo menos uma vez por ano ou com mais frequência em caso de alterações organizacionais importantes, alterações significativas na tecnologia, no objetivo dos negócios, alterações legais ou regulamentares, etc.

### 3.8. Aceitação dos Riscos

Após a elaboração do Plano de Tratamento, os Riscos Residuais, têm que ser aprovados pelo Conselho de Administração, e tem que se obter a aprovação dos responsáveis pelos riscos e a aceitação dos riscos residuais.

A aplicabilidade ou não aplicabilidade dos controles de segurança do Anexo A da norma ISO/IEC 27001, deve ser documentada na Declaração de Aplicabilidade. O Conselho de Administração deve aceitar todos os riscos residuais na Declaração de Aplicabilidade.