5. Avaliação do Risco e Planos de Contingência

1. Avaliação do risco e segurança

Este anexo serve para alertar o responsável do serviço/unidade funcional (UF) para ferramentas de gestão muito importantes e úteis na gestão da actividade do serviço/UF no âmbito do SIGIC, e cujo enfoque incide em 3 áreas:

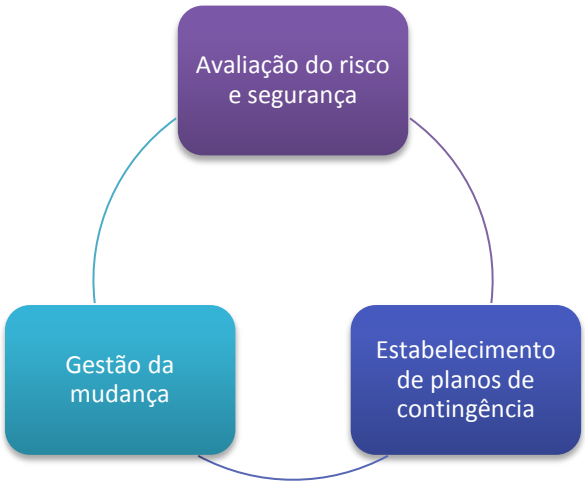

Ilustração 1: Relação entre a avaliação do risco e segurança, planos de contingência e gestão da mudança

O acompanhamento da actividade do serviço/UF deve ter em conta a avaliação dos riscos da respectiva actividade, quer para os profissionais, quer para o utente e para a organização como um todo. Tendo em conta a avaliação dos riscos, é necessário criar planos de segurança que minimizem o risco e planos de contingência que permitam gerir o impacto dos mesmos no serviço/UF, caso ocorram.

O SIGIC impõe mudanças, obrigando o serviço/UF a adaptar-se e a funcionar de acordo com um conjunto de normas que obrigam à alteração de processos, de atitudes e comportamentos por parte dos colaboradores. Logo uma boa gestão da mudança permite criar menos resistências e garantir o compromisso dos colaboradores no cumprimento das normas em vigor (leis, circulares normativas, etc.). A gestão da mudança está detalhada no Volume II do MGIC, área de gestão.

Tendo em conta os factores enunciados anteriormente, o responsável do serviço/UF deve incluir no seu modelo de monitorização da actividade do serviço/UF as ferramentas de gestão que garantem um melhor controlo da actividade, nomeadamente as relacionadas com a gestão do risco e a gestão da mudança.

2. Perspectiva do SIGIC

Não obstante a instituição hospitalar ter um sistema de avaliação e gestão do risco, o responsável do serviço/UF deve ter presente os riscos específicos, associados à actividade do sector que gere.

No âmbito de um serviço/UF os riscos podem ser de vários tipos, nomeadamente:

Risco laboral

- Risco associado aos profissionais do serviço/unidade funcional, nomeadamente o risco de contacto com agentes biológicos patogénicos, o contacto com objectos perfurantes, a contaminação por agentes tóxicos e corrosivos, exposição a agentes carcinogénicos, entre outros.

Risco para os utentes

- Risco associado aos utentes tratados pelo serviço/unidade funcional, nomeadamente o risco de infecções, acidentes traumáticos, erros na administração de fármacos, procedimentos terapêuticos ou diagnósticos inapropriados, entre outros.

Risco de incumprimento processual e do contrato

- Risco associado ao não cumprimento dos dispositivos normativos em vigor, nomeadamente o não cumprimento do regulamento do SIGIC, o não cumprimento do contrato programa, entre outros. No SIGIC os principais pontos de risco são o incumprimento das normas de inscrição na LIC, o agendamento (em relação à equidade no acesso e ao cumprimento dos TMRG), os registos de informação (em sistema apropriado, com qualidade, de forma atempada e de acordo com as regras vigentes) e a qualidade dos serviços prestados ao utente.

Risco financeiro

- Risco associado à sustentabilidade do serviço/UF e em última instância do SNS, nomeadamente o risco na rentabilização dos recursos humanos e físicos face aos serviços prestados, risco no retorno/valor esperado face ao custo dos investimentos realizados em recursos, risco na exploração intensiva de equipamentos dispendiosos, risco no aproveitamento das competências técnicas dos colaboradores, entre outros.

3. Considerações gerais sobre avaliação do risco

A avaliação do risco constitui a primeira fase da abordagem da gestão do risco dentro de uma organização e representa uma boa prática de gestão de qualquer actividade. Investir na sensibilização e na partilha de recursos, informações e boas práticas permite a prevenção dos riscos e produz um claro valor acrescentado para o serviço/UF.

É necessário adoptar uma abordagem integrada de gestão dos riscos que tenha em conta as diversas fases de avaliação dos riscos, as diferentes necessidades dos colaboradores e dos utentes e normas e planos institucionais.

As fases da avaliação do risco são as seguintes:

3.1. Análise dos Riscos

A análise de riscos é o processo pelo qual são relacionados os eventos, os impactos e avaliadas as probabilidades destes ocorrerem.

Na elaboração de uma análise de riscos, recomenda-se que sejam respeitadas as seguintes etapas:

Construção da Matriz de Impacto

A Matriz de Impacto é uma matriz que envolve um conjunto de itens que influenciam o dimensionamento do impacto no caso de ocorrência de uma determinada ameaça. A saber:

- Determinar os elementos críticos da actividade do serviço/UF que podem ser afectados por falhas e erros no processo;

Os elementos de maior impacto são os eventos clínicos e entre estes os actos cirúrgicos em que pela sua perigosidade intrínseca obrigam a um maior controlo (ver manual de cirurgia segura no Volume V).

- Levantar as ameaças/eventos decorrentes da execução dos passos do processo de actividade, que podem afectar ou causar um determinado impacto sobre algum elemento crítico da respectiva actividade do serviço/UF;

São ameaças reais em serviços/unidades funcionais cirúrgicos, por exemplo, a troca de identidade de um utente, a troca de um produto a administrar, a falha num equipamento num momento crítico, a desadequação da competência ou capacidade em relação ao acto prestado, a má gestão da cronologia dos eventos, entre outros.

- Definir o impacto para a actividade do serviço/UF no caso de ocorrência das ameaças/eventos.

Construção da Matriz de Probabilidade

Esta matriz evidencia aspectos que influenciam a probabilidade de ocorrência de uma determinada ameaça/evento. Na sua construção deve-se ter em conta os seguintes aspectos:

- Os pontos de controlo ou protecções existentes que podem prevenir ou minimizar a ocorrência das ameaças/eventos;

Por exemplo, os códigos de barras em utentes e produtos, redundância nas verificações de fases críticas, estabelecimento de protocolos, entre outros.

- As fraquezas ou fragilidades que podem existir nos respectivos controlos, de forma a obter uma avaliação da sua eficácia;

Por exemplo, dificuldades de medição, ausência de relatos de incidentes, inexistência de incentivos à participação de situações potenciadoras do risco, ausência de análise de acidentes, entre outros.

- A probabilidade da ameaça/evento vir a realizar-se devido a falha do controlo e o impacto previsto acontecer.

Por exemplo, o registo histórico fidedigno para determinar as ocorrências e respectivos impactos é um factor determinante.

A matriz de probabilidade deve conter as seguintes colunas:

Detalha-se de seguida o tipo de conteúdo que se pretende para cada coluna da matriz:

Tipo de ameaça

- O que pode correr mal

Exemplos de ameaças: amputou-se a perna errada, deflagrou um incêndio na enfermaria, administrou-se o fármaco ou tipo de sangue errado, o utente não reunia as condições para a cirurgia e o tempo operatório foi perdido, o utente inicia o tratamento numa fase já agravada da doença, um profissional contamina-se com um agente patogénico, o número de doentes tratados fica aquém do estabelecido no contrato, os utentes ultrapassam o TMRG em LIC, o número de reclamações é excessivo, a taxa de complicações excede as de prestadores congéneres, a degradação das condições de trabalho leva à fuga de colaboradores.

Elemento crítico da actividade

- O que pode ser afectado durante o desenvolvimento do trabalho

Exemplos: imagem institucional, qualidade da informação, segurança da informação, saúde do utente, motivação dos colaboradores, facturação da actividade, entre outros.

Impacto

- Qual o impacto esperado (1 – Alto, 2 Médio, 3 – Baixo)

O impacto deve ser medido em termos de:

- Custo financeiro;
- Custo social;
- Custo ético;
- Défice de sustentabilidade.

Controlo

- Qual a protecção existente

Exemplos: sistemas de monitorização activa, reuniões de discussão de incidentes e acidentes, protocolos, sistemas redundantes, auditorias internas aos processos, entre outros.

Vulnerabilidade

- Qual a eficácia do controlo

São necessários estudos para verificação da vulnerabilidade, incluindo simulações de acidentes.

Probabilidade

- Qual a possibilidade da ameaça se concretizar sobreutilizando o controlo (1 – Alto, 2 - Médio, 3 – Baixo)

A política relativa ao risco deve ser formalmente assumida. Ou seja, deve ficar expresso quais os níveis de risco em cada área que se entende adequado assumir, quais os riscos que de todo devem ser evitados, que riscos são transferidos (exemplo: através de seguros), entre outros.

Risco

- É o resultado da multiplicação do impacto versus a probabilidade

3.2. Definição dos Riscos

Esta etapa envolve a sumarização dos impactos relacionados e as suas respectivas probabilidades, para efeito de cálculo do risco real de um determinado evento (e o seu impacto) vir a ocorrer, consistindo nomeadamente em identificar:

- **As ameaças concretas** que sejam parte da realidade da organização;

Exemplos: adaptação do serviço/UF ao regulamento do SIGIC, a programas especiais como a Cirurgia Segura e o PTCO, etc.

- **Os controlos** (actividades, procedimentos, recursos ou responsabilidades existentes ou que possam ser construídos) que ajudam a reduzir ou a evitar a ocorrência da ameaça;

Exemplos: procedimento de *backup*, listagem de utentes a agendar de acordo com a prioridade clínica e tempo de espera, reuniões mensais da morbilidade e mortalidade, análise da conformidade com protocolos e comparação com resultados internacionalmente reconhecidos, etc.

- **As eventuais fraquezas dos controlos** indicados.

Exemplos: disponibilidade de recursos, sobrecarga de uso de equipamentos de tecnologia de informação, falta de validação da equidade nos agendamentos, ausência de registo das falências terapêuticas e complicações, etc.

3.3. Gestão dos Riscos

A gestão de riscos é um elemento central na gestão da estratégia de qualquer organização. É o processo através do qual as organizações analisam metodicamente os riscos inerentes às respectivas actividades, com o objectivo de identificar, estimar (probabilidade de ocorrência, impacto financeiro e outros) e controlar os mesmos, através de medidas para evitar, reduzir, assumir e/ou transferir os riscos para outra entidade.

A gestão de riscos deve ser um processo contínuo e em constante desenvolvimento, aplicado à estratégia do serviço/UF e à implementação dessa mesma estratégia. Deve analisar metodicamente todos os riscos inerentes às actividades passadas, presentes e, em especial, futuras do serviço/UF. Deve ser integrada na cultura da instituição hospitalar com uma política eficaz e um programa conduzido pelo responsável do serviço/UF. Deve traduzir a estratégia em objectivos tácticos e operacionais, atribuindo responsabilidades na gestão dos riscos a toda a organização, como parte integrante da respectiva descrição de funções. Esta prática sustenta a responsabilização, a avaliação do desempenho e respectiva recompensa, promovendo desta forma a eficiência operacional em todos os níveis da organização e criando uma imagem de responsabilidade social que se constitui um activo objectivo da organização.

4. Planos de contingência

4.1. Perspectiva do SIGIC

Ao ser efectuada a avaliação dos riscos e da segurança inerentes à actividade do serviço/UF, é necessário proceder à criação de protocolos de segurança e de planos de contingência no sentido de gerir o impacto dos riscos caso estes ocorram.

Assim, para os diversos tipos de risco da actividade do serviço/UF apresentados na parte relativa à avaliação do risco e segurança, devem existir protocolos de segurança, processos de controlo e planos de contingência, com as medidas a serem tomadas, as acções necessárias para implementar as medidas, os responsáveis por activar o plano e por implementar cada uma das medidas e a monitorização da actividade do serviço/UF até voltar aos seus padrões normais, de acordo com os dispositivos normativos institucionais e da tutela.

Por exemplo, no decurso da monitorização da equidade no agendamento dos utentes detecta-se um desvio à norma. Deve ser accionado o plano de contingência por risco de incumprimento processual (neste caso do regulamento do SIGIC), que accione as medidas a implementar (notificação dos responsáveis, verificação das causas, correcção dos fenómenos desencadeantes, etc.) para que seja restabelecida a equidade no agendamento, de acordo com a antiguidade e os níveis de prioridade clínica. Essas medidas podem ser de ordem processual (alteração dos processos de gestão dos episódios) em termos administrativos e clínicos, de ordem tecnológica como a adaptação dos sistemas de informação às regras de agendamento e de ordem cultural em termos de mudança da cultura e comportamentos dos colaboradores no processo de agendamento dos utentes.

Outro exemplo, a cirurgia a um utente complica-se e torna-se necessário intervenções para as quais a instituição hospitalar não tem competência. O plano de contingência deve assegurar que estando prevista esta eventualidade, estão estabelecidos protocolos com outras instituições no sentido de suprir as carências.

4.2. Considerações gerais sobre planos de contingência

Um plano de contingência, também designado por plano de riscos, plano de continuidade de negócios ou plano de recuperação de desastres, tem o objectivo de descrever as medidas a serem tomadas, incluindo a activação de processos manuais, para fazer com que os seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim a continuidade da disfunção ou uma paralisação prolongada que possa gerar maiores prejuízos ao serviço/UF e à instituição hospitalar, como a perda de utentes, perda de receita, sanções por parte da tutela, problemas jurídicos, exposição mediática, fuga de colaboradores para entidades concorrentes e até mesmo, em casos extremos, o encerramento do serviço/UF. Dada a grande importância deste processo, o seu custo deve estar incluído no orçamento do serviço/UF.

4.3. Criação de um Plano de Contingência

O plano de contingência deve ser desenvolvido envolvendo todas as áreas sujeitas a catástrofes, nomeadamente as naturais (incêndios, terramotos, inundações, etc.), biológicas (contaminações generalizadas por agentes patogénicos, etc.) informáticas, clínicas e administrativas. Todos os pontos do plano devem estar devidamente documentados e actualizados sempre que necessário. Também são necessários testes periódicos ao plano para verificar se o processo continua válido. O detalhe das medidas deve ser apenas o necessário para a sua rápida execução, sem excesso de informações que possam ser prejudiciais numa situação crítica.

O serviço/UF deve alinhar o seu plano de segurança com o da instituição hospitalar, nomeadamente no que se refere aos procedimentos mais simples de contingência na área dos serviços de informação que são: garantir a cópia de segurança regular das bases de dados, manter um '*site* de contingência' sempre actualizado, possuir ferramentas seguras para acesso aos dados remotamente para o caso de ser impossível chegar até às instalações do serviço/UF, ter redundância de servidores vitais para o funcionamento do serviço/UF (principalmente os que requerem muito tempo para reconstituição), manter senhas em local seguro mas de fácil acesso a pessoas chave do serviço/UF no caso de uma emergência, mudar as chaves de acesso (password) periodicamente para evitar acessos indevidos, encriptar a informação nas comunicações, manter antivírus e outras aplicações de segurança actualizadas.

Para criar um plano de contingência mais eficaz, o responsável do serviço/UF deve seguir as regras que se seguem, com algumas variações mínimas:

- Identificar todos os processos de actividade do serviço/UF;
- Avaliar os impactos na actividade, ou seja, para cada processo identificado, avaliar o impacto que a sua falha representa para o serviço/UF, levando em consideração também as interdependências entre processos. Como resultado deste trabalho é possível identificar todos processos críticos para a sobrevivência do serviço/UF;

Avaliar com a ajuda de gestores hospitalares o impacto financeiro dos riscos identificados.

- Identificar riscos e definir cenários possíveis de falha para cada um dos processos críticos, tendo em conta a probabilidade de ocorrência de cada falha, provável duração dos efeitos, consequências resultantes, custos inerentes e os limites máximos aceitáveis de permanência da falha sem a activação da respectiva medida de contingência;

Promover a discussão de ideias (*brainstorming*) com os colaboradores para identificar processos e riscos.

- Identificar medidas para cada falha, ou seja, listar as medidas a serem postas em prática caso a falha aconteça, incluindo até mesmo o contacto com a imprensa;
- Definir acções necessárias para operacionalização das medidas cuja implantação dependa da aquisição de recursos físicos e/ou humanos (por exemplo, aquisição de sinalização de emergência para situações de corte de energia eléctrica, colocação de carros de emergência com disfibrilhador nas enfermarias);
- Estimar custos de cada medida, comparando-os aos custos incorridos no caso de a contingência não existir;
- Definir forma de monitorização após a falha;
- Definir critérios de activação do plano, como tempo máximo aceitável de permanência da falha (por exemplo, a identificação de 2 ou mais utentes na enfermaria infectados com estirpes multirresistentes despoleta a intervenção da comissão de infecção, mais de 1 mês com infecções de repetição determina o encerramento provisório das salas afectadas para desinfecção);
- Identificar o responsável pela activação do plano, normalmente situado num alto nível hierárquico do serviço/UF ou da instituição hospitalar;
- Identificar os responsáveis em colocar em prática as medidas de contingência definidas, tendo cada elemento responsabilidades formalmente definidas e atribuídas. Deve também existir um substituto definido para cada elemento. Todos devem estar familiarizados com o plano de forma a evitar hesitações ou perdas de tempo que possam causar maiores problemas em situação de crise. A equipa responsável deve ter a possibilidade de decidir perante situações imprevistas ou inesperadas, devendo estar previamente definido o limite desta possibilidade de decisão;

- Definir a forma de reposição da actividade aos moldes habituais, ou seja, quando e como sair do estado de contingência e retornar ao seu estado normal de actividade, assim como quem são os responsáveis por estas acções e como este processo será monitorizado;

Promover simulações periódicas envolvendo todos os colaboradores.

- Gerir o processo de comunicação interna com o exterior ao longo de toda a crise (por exemplo, definir quem fala, quais as informações que são divulgadas, o resguardo da privacidade dos utentes e familiares, etc.).