6. Organização da Informação e Sistemas de Informação

1. Requisitos para criação de um serviço/unidade funcional no SIGLIC

Para a criação de um serviço/unidade funcional (UF) no SIGLIC, é necessário efectuar três procedimentos nas seguintes funcionalidades:

1. Criar o serviço/UF na ficha do hospital;
2. Mapear o serviço/UF criado com o serviço/UF do sistema de informação hospitalar (SIH) no Mapeamento de Serviços;
3. Registar os colaboradores do serviço/UF e especificar o tempo afecto a cada actividade no respectivo serviço/UF na Gestão de Colaboradores e Utilizadores.

2. Informação a ser actualizada pela instituição hospitalar

A fim de se garantir a qualidade dos registos na base de dados, a validade dos indicadores construídos com base nesses registos, a gestão eficaz das transferências de utentes e a gestão eficiente da LIC, é necessário que a UHGIC e os responsáveis de unidades funcionais (UF) garantam a actualização da informação na aplicação SIGLIC, directamente ou através do SIH, nomeadamente a seguinte:

- Documentos relativos ao utente e a eventos administrativos e clínicos;
- Formulários relativos a programas (PTCO, Oncologia, Cirurgia Segura, etc.);
- Ficha do hospital:
  - Dados gerais;
  - Capacidade instalada;
  - Gestão dos utilizadores do SIGLIC e respectivos perfis de acesso;
  - Serviços e contratos/convenções.
- Gestão do SIGIC e do Sistema de Informação (SI):
  - Gestão das não conformidades;
  - Mapeamentos entre os SIH e o SIGLIC.

Existem ainda outras funcionalidades do SIGLIC que a instituição hospitalar deve utilizar, nomeadamente a comunicação na rede para trocar informações com outras entidades integradas no SIGIC (hospitais do SNS e convencionados, URGIC e UCGIC), o cancelamento de notas de transferência e vales cirurgia (NT/VC) e a ferramenta que permite a simulação do cálculo do pagamento às equipas cirúrgicas em produção cirúrgica realizada em MRA.

Nos números seguintes, é descrito com maior detalhe o tipo de informação a ser actualizada e a sua importância em cada uma das funcionalidades do SIGLIC.

Para quaisquer esclarecimentos de como actualizar informação na aplicação SIGLIC devem consultar o manual de utilizador ou contactar o *helpdesk* do SIGLIC.

2.1. Eventos administrativos e clínicos

A instituição hospitalar deve registar no SIH ou directamente no SIGLIC todos os eventos, administrativos (colocação e eliminação de pendências) e clínicos (ex.: cirurgia) que constituem um episódio funcional, desde a referenciação até à sua facturação.

As UHGIC têm de garantir junto dos serviços e UF a actualização dos registos dos eventos de forma ao hospital cumprir os prazos em vigor sem incorrer em não conformidades.

Os serviços/UF devem garantir que os registos são efectuados não só com respeito pelos prazos legalmente em vigor, mas também com a qualidade desejada, cabendo ao seu responsável o dever de garantir que a informação foi registada correctamente no SI (vide anexo Gestão do processo clínico).

Para além de a informação ser integrada no SIGLIC, os respectivos documentos em suporte de papel devem constar do processo clínico do utente, à luz da legislação actual.

Tendo em conta que o registo e validação da conclusão do episódio são eventos de registo obrigatório no SI, o SIGLIC tem à disposição dos hospitais uma funcionalidade que permite efectuar estes registos para o caso de não os conseguirem efectuar no SIH.

Existe ainda uma funcionalidade à disposição dos hospitais do SNS que permite participar na gestão das transferências em operações como: o cancelamento de NT/VC, nos casos em que o utente se dirige à instituição hospitalar e expresse a sua vontade à respectiva UHGIC, através de documento escrito, de não utilizar o NT/VC. A instituição hospitalar deve providenciar a anexação do documento justificativo da recusa de transferência, assinado pelo utente, ao processo deste.

Em relação aos eventos clínicos, os serviços/UF devem preencher os respectivos impressos do SIGIC no SIH, como por exemplo os formulários do PTCO, das próteses e da Cirurgia Segura.

Para o efeito, é necessário que o responsável de serviço/UF diligencie no sentido dos locais, onde esses formulários devem ser preenchidos, estarem equipados com computadores com acesso à rede da instituição hospitalar, tais como as salas do BO e da consulta externa, e que os profissionais que vão preencher esses formulários tenham acesso aos SI. No caso do SIGLIC, têm que ter um utilizador e perfil de acesso a dados, adequado aos registos que têm de efectuar na aplicação.

O responsável de serviço/UF deve providenciar a existência de um banco de assinaturas, conforme norma da instituição hospitalar, que permita confirmar a relação entre a assinatura e o profissional autorizado a assinar documentos no âmbito do processo SIGIC.

2.2. Ficha do Hospital

A ficha do hospital é um ecrã do SIGLIC que tem por objectivo dotar os hospitais de um conjunto de funcionalidades que permite a gestão mais integrada e eficiente da LIC, quer no que se refere à capacidade instalada da instituição hospitalar, quer no que se refere à gestão dos serviços e respectivas UF.

A ficha do hospital disponibiliza informação que caracteriza os hospitais do SNS e convencionados do sector privado e social e permite determinar indicadores de produtividade relativos à actividade cirúrgica programada dos mesmos. Pretende-se ainda que esta informação facilite a criação de indicadores de procura e oferta de procedimentos cirúrgicos

no âmbito da cirurgia programada, ajustados à capacidade de cada hospital, a nível institucional, regional e nacional.

2.2.1. Dados Gerais

Na ilustração seguinte apresenta-se um resumo da informação que consta na Ficha do Hospital:

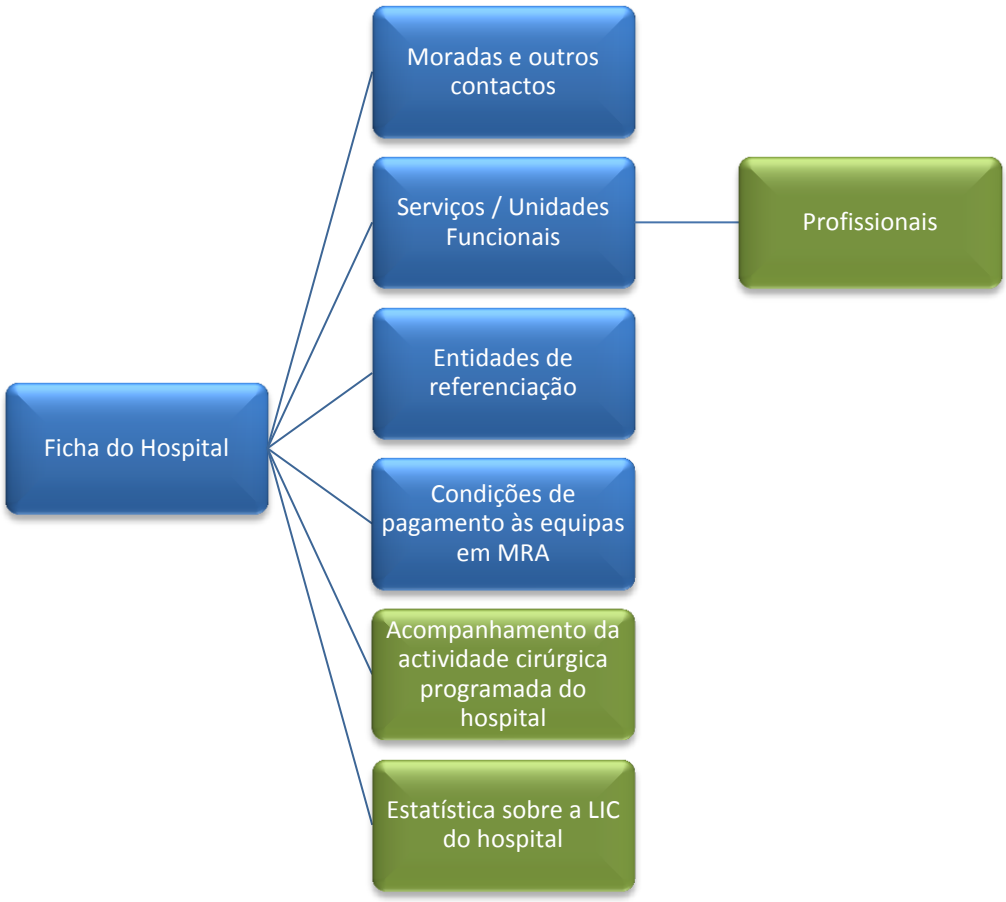


Ilustração 1 – Informação da Ficha do Hospital

Todas as pastas podem ser actualizadas localmente pela instituição hospitalar, à excepção das pastas a verde que são indicadores ou informação disponibilizados pelo SIGLIC, em função dos dados que constam na base de dados.

Cada pasta contém a seguinte informação:

Moradas e outros contactos	•Contactos oficiais do hospital no âmbito do SIGIC.
Serviços/UF	•Informação sobre serviços, UF, incluindo os respectivos profissionais e dados estatísticos que permitem o acompanhamento do contrato interno (MRA e MRC) negociado entre o Responsável do Serviço/UF e o CA. Em relação aos profissionais associados a um Serviço/UF, correspondem todos os médicos que propõem utentes para cirurgia e os chefes de equipas cirúrgicas (cirurgiões principais).
Entidades de referenciação	•Informação sobre as entidades públicas ou privadas que referenciam utentes para o hospital (centros de saúde, hospitais, clínicas, etc.).
Condições de pagamento às equipas em MRA	•Informação sobre as condições específicas de pagamento às equipas cirúrgicas em actividade cirúrgica programada realizada em MRA. Esta funcionalidade, juntamente com a definição das equipas-tipo, permite simular o pagamento aos colaboradores das equipas cirúrgicas contratados pela instituição para trabalhar em regime MRA. Esta ferramenta é possível de parametrizar pelo utilizador e está disponível caso o hospital tenha interesse em utilizá-la.
Acompanhamento da actividade cirúrgica programada do hospital	•Conjunto de indicadores do hospital, a uma determinada data, sobre registo da actividade cirúrgica programada, em ambulatório e em internamento, e sobre a produção realizada face à contratada no âmbito do acompanhamento do contrato-programa do hospital com a ACSS.
Estatística sobre a LIC do hospital	•Conjunto de indicadores sobre a actividade cirúrgica programada do hospital, nomeadamente sobre LIC, operados, produção cirúrgica em MRA e MRC, cancelados, transferidos, devolvidos, entre outros.

A UHGIC deve garantir a actualização da ficha do hospital, cabendo aos responsáveis de serviço/UF validar a informação registada na aplicação e reportar à UHGIC possíveis erros para correcção.

Em relação às moradas e outros contactos na Ficha do Hospital, é obrigatório a criação e actualização por parte da UHGIC dos seguintes endereços electrónicos:

- sigic@domínio da instituição hospitalar;
- Coordenador da UHGIC da instituição hospitalar;
- Director Clínico da instituição hospitalar.

É também obrigatório que os endereços electrónicos, telefone e fax relativos à UHGIC, coordenador da UHGIC e conselho de administração (CA) sejam criados e actualizados na Ficha do Hospital.

No caso de existirem na instituição hospitalar cirurgiões que efectuem propostas sem reportarem a um serviço/UF em particular, a UHGIC deve, no seu SIH e no SIGLIC, constituir a ficha de um serviço sob a responsabilidade directa do Director Clínico, que deve validar as propostas constituídas ao abrigo do mesmo e ser o responsável pelo correcto agendamento dos utentes da respectiva LIC ou integrá-los num outro serviço/UF cirúrgico, independentemente da especialidade dos cirurgiões.

Os médicos proponentes e os chefes das equipas cirúrgicas devem estar obrigatoriamente associados aos respectivos serviços/UF, podendo ser incluídos outros profissionais do serviço/UF. A gestão destes colaboradores é efectuada no ecrã de gestão de colaboradores/utilizadores, na aplicação SIGLIC.

2.2.2. Capacidade instalada

A capacidade instalada é um ecrã do SIGLIC através do qual deve ser recolhida informação actualizada sobre os recursos humanos e físicos envolvidos na actividade cirúrgica da instituição hospitalar. A informação solicitada está organizada de acordo com a sua classificação, tipologia ou agrupamento definidos pelo Ministério da Saúde.

A informação está organizada na seguinte forma:

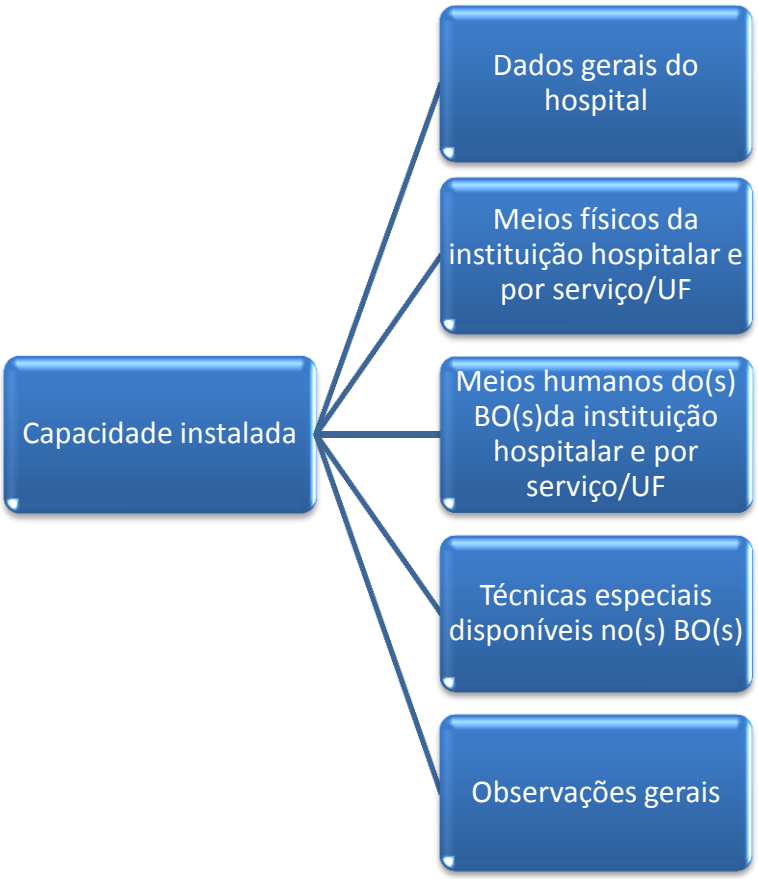


Ilustração 2 – Informação sobre a Capacidade Instalada

A pasta da capacidade instalada contém informação da instituição hospitalar relativa aos meios humanos e físicos disponíveis para realizar a **actividade cirúrgica programada**, caracterizada por serviço/UF. No contexto do SIGIC, o serviço/UF deve ser entendido como o conjunto de meios humanos e físicos, afecto ao diagnóstico, tratamento e recuperação de doentes, organicamente constituído, dirigido e gerido por um director/responsável. Não pode ser confundido com um sector ou uma unidade de internamento. Existindo UF na dependência do serviço cirúrgico, os recursos e resultados de cada uma são considerados na análise global do serviço. A lógica subjacente a esta formulação baseia-se na responsabilidade do coordenador da UF que responde pela actividade do seu sector, embora o director de serviço seja o responsável último pela actividade global do serviço, incluindo a que ocorre nas suas diversas UF. Os custos e os recursos são analisados em função das responsabilidades de gestão instituídas. Por exemplo, num serviço de cirurgia geral pode existir uma UF de cirurgia da obesidade, cujo responsável tem ao seu dispor os recursos humanos e físicos afectos à unidade e responde pela execução do processo de prestação de cuidados e pelos resultados. O director do serviço responde, por sua vez, por toda a actividade, incluindo a que ocorre na UF de cirurgia de obesidade.

Os dados da capacidade instalada devem reflectir a média do ano a que correspondem e devem ser actualizados em Julho e em Janeiro, referindo-se respectivamente aos dados do 1º semestre do ano em curso e à média dos recursos disponíveis no ano anterior.

Cabe à UHGIC garantir a actualização dos dados da capacidade instalada da instituição hospitalar, sendo da responsabilidade do director de serviço/UF validar os dados relativos ao seu serviço/UF e promover a sua correcção e actualização junto da UHGIC.

Cada pasta contém a seguinte informação:

Dados gerais do hospital	•Indicadores sobre os recursos físicos e humanos da instituição hospitalar como um todo, nomeadamente o nº de profissionais, a lotação de camas, a disponibilidade de serviços de MCDT e de tipos de Urgências.
Meios físicos do hospital e por Serviço/UF	•Informação sobre os recursos físicos da instituição hospitalar como um todo e por serviço/UF cirúrgico, nomeadamente sobre o nº de camas, nº de salas, nº horas disponíveis das salas, disponibilidade das salas do BO por tipo de produção (MRA e MRC), salas exclusivas para ambulatório e urgência, entre outros.
Meios humanos do(s) Bloco(s) do hospital e por Serviço/UF	•Informação sobre os recursos humanos do hospital ao nível do(s) BO(s) e por Serviço Cirúrgico/UF, nomeadamente a disponibilidade em termos de horas de trabalho dos colaboradores por grupo profissional (médicos, enfermeiros, auxiliares e administrativos) em cada Serviço/UF e no BO.
Técnicas especiais disponíveis no(s) BO(s)	•Lista de recursos técnicos instalados e em funcionamento na instituição hospitalar , em particular o equipamento de diagnóstico e terapêutica, permitindo avaliar a sua capacidade técnica disponível e, consequentemente, garantir a adequada transferência de utentes entre hospitais. Esta informação é essencial para que seja possível realizar as transferências dos utentes para os hospitais que possuam as técnicas peri-operatórias necessárias ao tratamento dos mesmos.
Observações gerais	•Informações adicionais sobre a capacidade instalada na instituição hospitalar que não constam nas restantes pastas. Por exemplo, o hospital faz subcontratação de médicos anestesistas para suprir as suas necessidades ou apenas uma sala do BO está equipada com material para microcirurgia.

A informação sobre os recursos humanos dos vários grupos profissionais do serviço/UF e do(s) BO(s) da instituição hospitalar tem como unidade de medida o número total de horas semanais de trabalho afectos ao serviço/UF, incluindo os períodos de atendimento não programado e os afectos à urgência interna quando esta não é assegurada pelo serviço de urgência (inclui o número médio de horas extraordinárias prestadas no serviço/UF). O número total de horas semanais deve ser distribuído pelos sectores de actividade – Consulta de

Cirurgia, BO e outros - de acordo com os horários de trabalho aprovados pelo CA da instituição hospitalar.

Tratando-se de profissionais que prestam apoio a vários serviços/UF sem número de horas fixo em cada um, a instituição deve atribuir um número médio de horas de trabalho afectas a cada um dos serviços/UF, com base no número de actos ponderados efectuado ou número de utentes a cargo por unidade de tempo.

2.2.3. Carteira de serviços, contratos e convenções

Os responsáveis de serviço/UF devem garantir o registo actualizado, na aplicação SIGLIC ou no SIH, da sua carteira de serviços, ou seja o conjunto de procedimentos que o serviço/UF tem capacidade de efectuar, tendo em conta os seus recursos físicos (equipamentos, número de camas, etc.), condições especiais (exemplo: a instituição dispõe de unidade cuidados intensivos ou não, estão disponíveis outras valências eventualmente necessárias ou não, etc.) e as competências dos seus colaboradores.

Cabe ao CA da instituição hospitalar garantir que a informação relativa ao contrato interno de produção cirúrgica nos regimes MRA e MRC negociado com os serviços/UF, no caso dos hospitais do SNS, ou relativa à convenção assinada com as ARS, no caso dos hospitais do sector social e privado, está registada correctamente no SIGLIC.

Cabe à UHGIC actualizar a informação no SI relativa à carteira de serviços e contratos internos ou convenções da instituição hospitalar por serviço/UF, envolvendo e promovendo acções de sensibilização junto dos responsáveis de serviço/UF para este fim. A UHGIC é também responsável por comunicar às URGIC/UCGIC as respectivas alterações.

Através do conhecimento da carteira de serviços de cada serviço/UF o hospital, e as unidades de apoio regionais e central podem avaliar a adequação da oferta face à procura de serviços por parte dos utentes e, consequentemente, ajustar melhor a capacidade instalada do serviço/UF à procura existente. É possível ainda o serviço/UF, no caso de ter excedentes a nível de capacidade instalada, aproveitar melhor os seus recursos através da disponibilização para receber por via de transferência utentes de outros hospitais, assinalando na sua carteira de serviços quais os procedimentos disponíveis para os utentes do exterior e qual o número médio de transferências registadas no serviço/UF por mês.

2.3. Mapeamentos entre o SI local e central

Os mapeamentos entre o sistema central e local permitem às instituições a comunicação numa linguagem universal, garantindo não só que todos os conteúdos têm uma interpretação única nas relações inter-institucionais no âmbito do SIGIC, mas também a a qualidade dos registos e respectiva classificação de acordo como as regras do SIGIC.

Os mapeamentos entre os sistemas de informação locais das instituições (exemplo: SONHO, SAM, etc.) e o central (SIGLIC) são cruciais para assegurar a qualidade da informação recolhida para a base de dados central do SIGIC.

É necessário que a UHGIC garanta, com o apoio dos responsáveis de serviço/UF, a actualização sistemática dos mapeamentos entre os SIH e o SIGLIC, nomeadamente os motivos de cancelamento do episódio, os motivos de cancelamento da cirurgia, os motivos de cancelamento do agendamento, os destinos após alta, os tipos de programação cirúrgica, os motivos de pendentes, os subsistemas de saúde e os códigos de diagnósticos e de procedimentos.

Os mapeamentos interferem na forma como os dados são geridos na base de dados central, reflectindo-se e nos indicadores da instituição, pelo que devem ser validados quer pela coordenação da UHGIC, quer pelos responsáveis de serviços/UF.

Para exemplificar a importância dos mapeamentos entre os sistemas de informação local e central, apresenta-se de seguida o caso do **mapeamento de serviços/UF**.

O mapeamento de serviços consiste numa funcionalidade que permite à instituição hospitalar manter, por um lado, as suas designações no SIH, tendo em conta as suas necessidades específicas (centros de custo, áreas funcionais, etc.) nomeadamente ao nível dos serviços (cirúrgicos e médicos) e, por outro lado, estabelecer uma relação com os serviços/UF oficialmente constituídos na aplicação SIGLIC, permitindo a correcta integração de dados entre os dois sistemas.

A instituição hospitalar pode atribuir a um mesmo serviço/UF, conforme as actividades (consultas, internamentos, técnicas), várias designações no seu SIH, sendo obrigatório que todas as designações correspondam a um serviço ou UF designado no SIGLIC.

O SIGLIC prevê a existência de UF. Estas não podem ser confundidas com unidades orgânicas (serviços). As UF são obrigatoriamente constituídas sob a tutela de um serviço (unidade orgânica) e correspondem à existência de um conjunto restrito de recursos afectos a um conjunto específico de procedimentos/patologias, que condiciona a capacidade de resposta da instituição hospitalar. Por exemplo, num serviço de 10 cirurgiões, em que só 2 estão habilitados para cirurgia digestiva por via laparoscópica, tendo em conta a lista de inscritos e a impossibilidade de realocar recursos, pode verificar-se alguma incapacidade objectiva do serviço em satisfazer toda a procura, por ordem cronológica de inscrição e por prioridade. Nestes casos, deve ser criada uma UF para contornar a mais que provável penalização do serviço, por registo de uma não conformidade em matéria de equidade do agendamento. Importa pois reforçar que sempre que a instituição hospitalar crie um novo serviço ou UF no seu SIH, tem de posteriormente criar o seu mapeamento com um dos serviços já existentes na aplicação SIGLIC.

Os serviços e unidades que não estão mapeados com o sistema central, estão bloqueados no que se refere à integração dos dados e, consequentemente, ficam excluídos da sua representação no SIGLIC.

A instituição hospitalar e em particular os membros da UHGIC e os directores de serviço ou os responsáveis de UF têm de garantir a protecção da informação dos utentes e o acesso a esta apenas por agentes credenciados, legalmente habilitados à utilização da mesma. Por princípio, só deve ter acesso à informação de um utente quem, no legítimo exercício das suas funções, tiver necessidade de acesso. A instituição hospitalar deve definir políticas de utilização da informação, escritas e adequadamente divulgadas. Os sistemas de informação utilizados devem ter mecanismos de controlo que promovam essas políticas.

2.4. Gestão de colaboradores e utilizadores do SIGLIC

Todos os colaboradores que sejam utilizadores do SIGLIC e ainda os registados como participantes nos eventos inseridos no SI do SIGIC têm de estar inscritos na ficha de colaboradores. A finalidade desta inscrição prende-se, por um lado, com a determinação dos participantes nos eventos (consultas, internamentos, técnicas) e, por outro, com a verificação do perfil adequado às funções desempenhadas.

2.4.1. Segurança e perfis de utilização

A informação sensível do utente é protegida na aplicação SIGLIC através de um sofisticado sistema de gestão de colaboradores e utilizadores e respectivos perfis de acesso à informação, constante da base de dados central, que visa garantir que só utilizadores credenciados possam aceder à informação, e que esta é disponibilizada em função do nível de acesso de cada um.

O SIGLIC incorpora um conjunto de dispositivos que procura garantir um acesso criterioso à informação do utente, tendo por base a necessidade funcional dos utilizadores no acesso à informação e a separação de conteúdos, para que os registos clínicos só sejam acedidos por pessoal qualificado.

Em termos de perfis de acesso à informação, os colaboradores e utilizadores associados a uma instituição hospitalar só podem consultar e gerir os dados da sua instituição. É da responsabilidade desta definir no SIGLIC o perfil para cada utilizador. Os colaboradores de cada serviço/UF só devem ter acesso à informação de utentes inscritos nos respectivos serviços/UF no âmbito de eventos formalmente estabelecidos e na extensão das suas competências. Quando em funções no serviço de urgência, acedem aos utentes que são admitidos nesse serviço ou aos internados na instituição hospitalar.

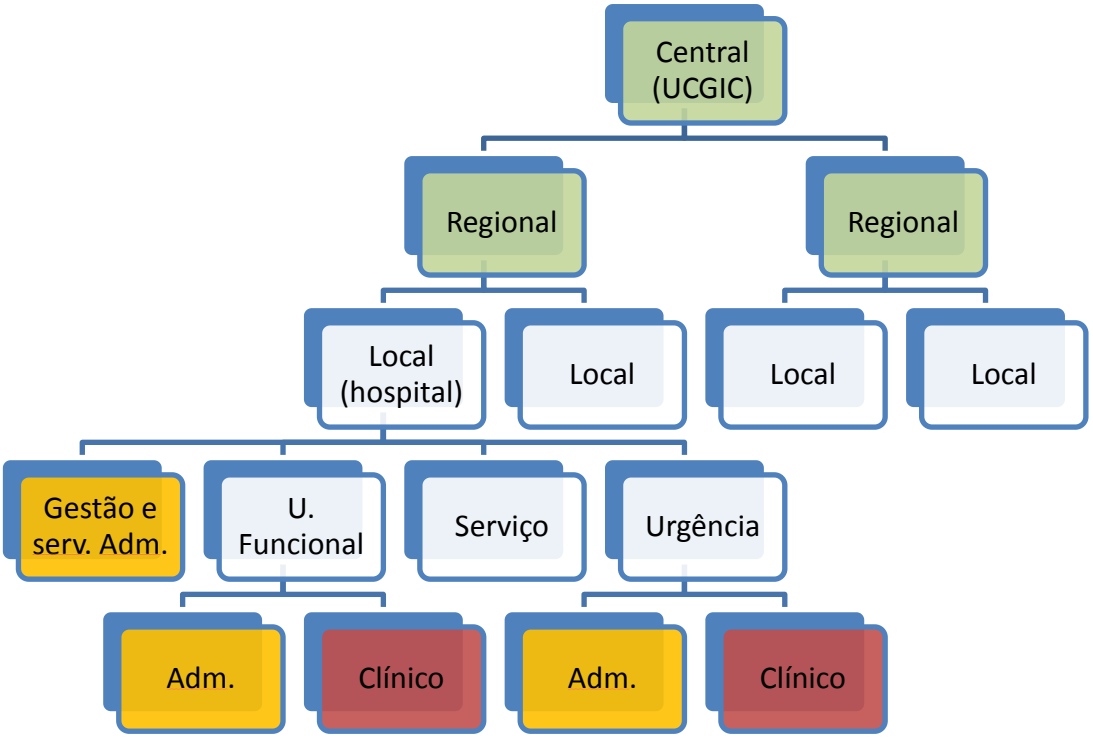


Ilustração 3 – Níveis de Acesso à Informação no SIGLIC

É importante garantir que todos os colaboradores que intervêm na actividade do SIGIC da instituição hospitalar e necessitam de consultar ou registar informação no SIH ou central (SIGLIC), tenham acesso e perfil adequado na aplicação às funções que desempenham no processo de gestão do utente.

O responsável do serviço/UF deve definir os colaboradores que têm de ter acesso aos sistemas de informação locais e central, nomeadamente ao SIGLIC, quais os respectivos perfis de acesso adequados, ou seja o nível de abrangência da informação que podem consultar, quais os registos que podem efectuar e que devem ser criados no SIGLIC. Os perfis dos utilizadores podem sempre ser ajustados face às necessidades do serviço/UF.

Aos chefes de equipas cirúrgicas deve ser atribuído o estatuto de utilizador no SIGLIC para que possam confirmar nesta aplicação os registos que efectuaram no SI local.

Devem também ser registados como colaboradores, todos os profissionais que integram as equipas cirúrgicas, independentemente da modalidade de produção cirúrgica

(MRA ou MRC). Para cada colaborador deve ser especificado os serviços/UF a que está afecto e a percentagem de tempo afecto a cada actividade em cada um deles.

O SIGLIC permite aos hospitais definir localmente os colaboradores e utilizadores da aplicação SIGLIC e os respectivos perfis de consulta e de registo de informação, assim como efectuar a gestão dos utilizadores e colaboradores autonomamente, com recurso aos serviços do helpdesk, apenas para esclarecimento de dúvidas operacionais que possam surgir.

O registo da informação pode ter implicações graves ao nível da gestão de recursos, ao nível financeiro, ao nível de planeamento e ao nível de gestão de utentes. O melhor controlo da qualidade da informação registada é aquele que é realizado pelos responsáveis directos pela mesma, pelo que devem ter acesso à mesma e serem incentivados a validá-la.

2.5. Comunicação na rede

A comunicação na rede é um ecrã da aplicação SIGLIC que permite à instituição hospitalar comunicar com outras entidades do SIGIC, nomeadamente as UHGIC dos hospitais do SNS e do sector privado e social convencionados, URGIC e UCGIC. O utilizador pode consultar, registar e responder a comunicações entre a entidade, à qual está associado o seu perfil de acesso, e as restantes entidades do SIGIC, quer na perspectiva de emissor do pedido, quer na de destinatário. Assim, o utilizador tem acesso não só aos pedidos que criou, como também aos pedidos que lhe são dirigidos por outras entidades.

A utilização desta funcionalidade é obrigatória para o registo de todas as comunicações entre as entidades do SIGIC. Como exemplo, os pedidos entre hospitais de origem e de destino no âmbito das transferências de utentes, o pedido por parte do hospital de destino (HD) do processo do utente e MCDT ao hospital de origem (HO), a sinalização de qualquer matéria processual no SIGIC, bem como quaisquer disfunções no SI central ou nos interfaces que tenham impacto na actividade e nas normas do SIGIC, com particular importância nos casos em que daí possam decorrer não conformidades. A contestação de uma não conformidade baseada na inoperância do SI central deve referir o número da comunicação na rede onde tal foi reportado.

2.6. Simulador do cálculo do custo das equipas cirúrgicas em MRA

Uma das possibilidades processuais no SIGIC é a opção de, nos termos regulamentares, efectivar as cirurgias com equipas cirúrgicas pagas em função das cirurgias efectuadas – Modalidade Remuneratória Alternativa (MRA).

Existe na aplicação SIGLIC uma ferramenta que permite à instituição hospitalar calcular valores indicativos a pagar aos colaboradores das equipas cirúrgicas, que realizam actividade cirúrgica programada em regime MRA, em função das parametrizações para cada serviço/ UF, introduzidas pela instituição hospitalar.

Caso o responsável do serviço/UF pretenda utilizar esta ferramenta, necessita definir na aplicação as equipas tipo e as condições de pagamento negociadas com o CA, ou seja, qual o pagamento a efectuar em MRA, em percentagem ou valor, aos colaboradores das equipas cirúrgicas de acordo com a sua função na equipa.

A portaria n.º 852/2009, de 7 de Agosto, que regulamenta o valor e as regras da produção cirúrgica adicional realizada no âmbito do SIGIC, aponta para que as equipas em MRA sejam pagas em função dos preços dos GDH definidos naquela portaria.

O responsável do serviço/UF pode introduzir na ficha do hospital condições adicionais para o pagamento às equipas cirúrgicas, incrementando ou diminuindo o valor base em função do diagnóstico, ou do procedimento cirúrgico, ou do GDH gerado, ou ainda em condições especiais como por exemplo a utilização de sangue no BO. Às condições definidas é atribuído um factor (percentagem) que faz variar o valor a pagar à equipa cirúrgica. Uma condição adicional pode consistir, por exemplo, em estabelecer que o valor a pagar às equipas cirúrgicas em MRA terá um acréscimo de 10%, sempre que as cirurgias realizadas gerem o GDH 160 e o procedimento realizado seja codificado com o código 5369 e o diagnóstico com o 55329.

Esta ferramenta permite a disponibilização de diversos indicadores e relatórios no SIGLIC que podem ser utilizados, não só na gestão dos pagamentos às equipas cirúrgicas, mas também no acompanhamento da própria actividade cirúrgica programada de cada serviço/UF e da instituição hospitalar, quer em termos financeiros, quer de produção.

3. Indicadores e relatórios disponibilizados pelo SIGLIC

A aplicação SIGLIC tem ao dispor da UHGIC e dos responsáveis de serviço/UF indicadores sobre a LIC, produção cirúrgica e financeiros que permitem a monitorização da satisfação da procura e cumprimento dos TMRG, o acompanhamento do contrato programa da instituição hospitalar, o acompanhamento da produção realizada em MRA e MRC por serviço/UF, o valor a facturar por episódio funcional e o valor a pagar às equipas cirúrgicas em regime MRA, entre outros.

A UHGIC e os responsáveis de serviço/UF devem, através da consulta regular do SIGLIC, analisar os relatórios dos indicadores e reportar na comunicação na rede quaisquer disparidades encontradas. A falta de comunicação nestes termos de eventuais erros, omissões ou imprecisões detectadas, equivale à aceitação tácita dos indicadores observados e à co-responsabilidade na publicação dos mesmos.

4. Qualidade e segurança nos sistemas de informação

Este capítulo destina-se a alertar a instituição hospitalar para medidas que deve tomar de forma a garantir a qualidade e segurança da informação, nomeadamente no acesso à informação.

4.1. Qualidade em SI

4.1.1. Considerações gerais sobre qualidade

Na óptica de SI, o ponto fundamental para que um sistema seja considerado de qualidade é a coerência da sua informação. As informações que o SI contém são coerentes quando reflectem a realidade, ou seja, a actividade real da instituição hospitalar. Para tal é necessário garantir que o SI foi modelado de forma coerente com essa mesma realidade. No caso dos hospitais, a realidade que pretendemos medir é primeiramente a actividade clínica, ou seja, a interacção entre a instituição e o utente, centrada na procura da resolução de problemas de saúde.

A informação do SI tem que ser igualmente consistente. Os SI bem desenhados usam redundância para poder verificar a consistência, que diz respeito ao relacionamento de integridade das informações registadas. Essa redundância é desenhada de forma que a informação redundante seja provida por diferentes fontes. A detecção de inconsistência na informação é um alerta para a possível presença de incoerência.

Ilustração 4 – Coerência e consistência nos SI

A consistência da informação pode ser verificada pelo SI, enquanto a coerência da mesma precisa de ser validada pelos colaboradores da instituição hospitalar que são os utilizadores da informação. O SIGLIC explora activamente este conceito, recolhendo dados de diversos parceiros distintos (utentes, clínicos, administrativos) relativos à mesma realidade. A confrontação destes dados permite determinar a consistência da informação. No SIGLIC a

consistência da informação também é observada ao longo do tempo, ou seja, a mesma realidade é observada e registada em tempos diferentes, integra-se a mutação esperada decorrente da evolução e determina-se de novo a consistência da informação.

A qualidade da informação nos SI tem ganho uma enorme importância nas organizações nos últimos anos. Na saúde este aspecto é particularmente importante pois, ao promovermos a mudança de paradigmas em que a informação de escrita passa a digital, o financiamento baseado no histórico passa a ser baseado em informação, em que as decisões passam de assentes na confiança depositada em pessoas, para assentes em factos medidos e registados. É necessário garantir que a informação é de total confiança, sob pena de serem prestados os cuidados de saúde errados, serem tomadas decisões de gestão erróneas e as instituições serem financiadas inadequadamente.

Os problemas com a qualidade da informação são sentidos de forma rotineira por todas as instituições, nomeadamente as hospitalares, com diferentes níveis de gravidade e de prejuízo. O impacto negativo traduz-se em custos desnecessários, processos de decisão afectados ou na perda de confiança dos utentes.

Todos os intervenientes no processo SIGIC, sejam eles consumidores, fornecedores ou produtores de informação, desempenham um papel no processo de criação de valor. Um SI, à luz deste enquadramento, não é mais do que um processo de transformação de informação, cujo sucesso depende do grau de satisfação dos consumidores dessa informação. São consumidores da informação gerada em saúde e em particular no SIGIC os utentes, profissionais de saúde, gestores, decisores políticos, cientistas e a sociedade em geral com particular enfoque nos contribuintes que sustentam o sistema.

A informação é hoje encarada como um recurso essencial para as organizações, mas só nos últimos anos é que se reconheceu a sua importância estratégica. O seu reconhecimento como recurso significa que tem que ser gerida como tal, que é necessária a existência de uma estrutura capaz de assegurar que a informação esteja disponível no momento, na forma e na quantidade desejável para os seus consumidores, ou seja, que tenha qualidade. A qualidade da informação no SI é essencial para que seja possível produzir informação que seja útil e relevante para a gestão.

Todas as decisões que se tomam, são baseadas num conjunto de informações que está disponível no processo de tomada de decisão. A decisão final depende das características da informação que lhe serviu de *input*. Informação com défice de qualidade não conduz à tomada de decisões adequadas que, quando aplicadas, produzam os resultados esperados.

Assim, a informação de qualidade deve ter as seguintes características:

Ilustração 5 – Características da qualidade em informação e SI

Todas estas características têm que estar presentes para existir qualidade na informação. Os dados do SI devem ser correctos (ter objectividade, correcção, reputação e veracidade), ser sustentáveis (identificando os seus autores e respectivos enquadramentos, a data a que se referem, conterem elementos destinados à determinação da coerência e consistência), ter relevância (valor acrescentado, volume apropriado, completos, disponíveis), ser actuais (disponibilizados em tempo útil), apresentáveis (compreensivos, consistentes, concisos e de fácil interpretação), acessíveis (disponíveis no tempo certo no sítio certo), adaptáveis (por forma a poderem ser traduzidos e apresentados na medida das necessidades, competências, cultura e capacidade de cada grupo de utilizadores) e seguros (tem de existir a garantia da sua preservação física ao longo do tempo, de que só é acedida por quem de direito, que não é adulterada, que todas as modificações identificam os seus autores e determinam a datas e as circunstâncias em que ocorreram). Desta forma garante-se a qualidade da informação que é gerada a partir do tratamento desses dados. Apartir daí, a instituição hospitalar pode aumentar a capacidade para utilizar essa informação, ou seja, aumentar o seu conhecimento relativamente à realidade da instituição, utilizando a informação nos seus processos de decisão.

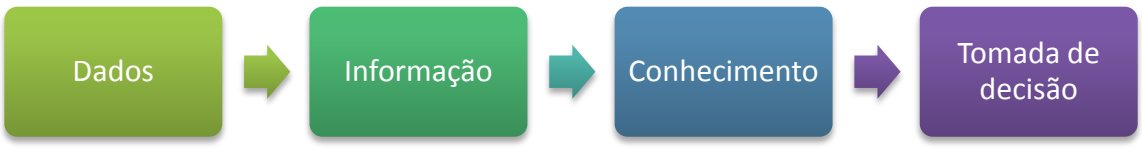


Ilustração 6 – Fluxo de informação para a tomada de decisão

Um conjunto de dados pode estar correcto, mas a sua apresentação dificultar a sua compreensão ou não estar disponível em tempo útil. Estes aspectos diminuem a qualidade da informação junto do utilizador.

As consequências da falta de qualidade na informação são várias: erros médicos, falhas nos processos, erros de comunicação, custos acrescidos devido ao impacto que causam e os custos da sua reparação, a perda da confiança dos utentes e colaboradores da instituição hospitalar, processos de tomada de decisão afectados, motivação das equipas diminuída ou processos de reestruturação organizacional, como a certificação, limitados pelo acesso a informação pouco "utilizável". A título de exemplo refira-se que, segundo a American Medical Association, 120.000 cidadãos americanos morrem por ano devido a erros nos diagnósticos, muitos destes poderão ter na origem ou como contributo informação de má qualidade. Uma das áreas de particular importância é a de controlo de qualidade e de segurança que permite antecipar e evitar acidentes de consequências nefastas. Estas áreas dependem primordialmente de informação qualificada.

Por outro lado, lidar com a qualidade da informação implica uma mudança de atitude para com este problema. Não é mais um problema de tecnologia mas sim um problema de gestão, de engenharia ou mesmo de governação. A tendência de considerar a informação como algo que está nas bases de dados, e, por conseguinte, da responsabilidade de um hipotético departamento de informática, tem de dar lugar ao reconhecimento da informação como um recurso essencial primariamente da responsabilidade da área do negócio. Significa no caso concreto na área da saúde e da prestação de cuidados, que necessita de uma estratégia adequada, enquadrada numa missão, centrada na visão, traduzida num plano e com recursos alocados à sua execução.

Um SI pode ser considerado como o conjunto gerido de recursos humanos e materiais, destinados a realizar as actividades de adquirir, armazenar, processar e difundir informação, quer estejam ou não envolvidos computadores. A sua missão é a de fornecer informação com qualidade a quem dela necessita, a agentes internos ou externos à organização em causa.

A qualidade da informação é uma dimensão do sucesso do SI. Deste modo, a qualidade da informação é um elemento primordial a considerar na avaliação da qualidade do SI, a par de outros elementos, como seja a qualidade das infra-estruturas, das aplicações e do serviço de suporte.

Resumindo, as organizações têm diferentes níveis de requisitos de qualidade na informação que utilizam, pelo que devem tomar medidas adequadas a esses níveis. Qualquer actuação para identificar, resolver e prevenir problemas na informação implica um custo que será compensado pela melhoria conseguida.

Gerir a qualidade da informação será equilibrar o peso que se está disposto a suportar para obter o nível desejado de qualidade, mas procurar sempre fazer mais com menos. A instituição deverá então lançar um programa com as dimensões adequadas ao peso do seu problema. Esta adequação traduzir-se-á no âmbito das medidas a tomar, nos contornos do sistema a implementar e no valor dos recursos a adquirir.

É importante salientar portanto a necessidade da inclusão da qualidade da informação no âmbito das actividades de planeamento de SI da instituição. A política da qualidade da informação a adoptar é algo que tem a sua origem no topo da gestão, fruto dos processos de decisão estratégicos. No entanto, este tema encontra-se ausente da maior parte das abordagens para o planeamento de SI, actividade que surge direccionada mais para a identificação da arquitectura do SI e para a identificação das aplicações a instalar.

4.1.2. Modelo para a garantia da qualidade

Um SI adquire informação (ou dados) e transforma-os em mais informação, para posterior disponibilização aos utilizadores. Para poder monitorizar a qualidade da informação, é necessário compreender o ciclo de vida da informação. Basicamente, a informação é recolhida, processada, armazenada e mais tarde consultada para ser utilizada. Três ciclos podem ser identificados, o ciclo de aquisição, o de processamento e o de utilização.

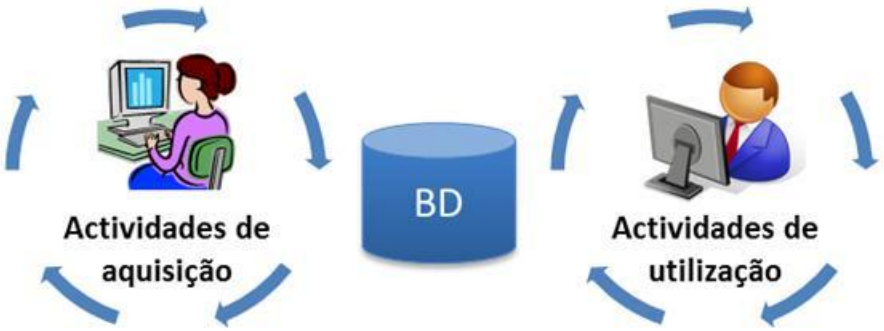


Ilustração 7: Ciclo de vida da informação

O ciclo de aquisição tem com pressuposto a definição do modelo conceptual de dados que define a visão do mundo real que deve ser recolhida e esclarece quando, como, em que circunstâncias, porque meios. Inicia-se com a aquisição de dados, prossegue com a validação dos dados e sua qualificação em termos de consistência, face a outros existentes e face a padrões estabelecidos por fim o seu armazenamento. No caso dos sistemas centrais do SIGIC os dados são recolhidos dos sistemas de produção para evitar duplicação de esforço, e são validados e qualificados em função da sua consistência, este ciclo incorpora um sistema de retorno de informação sobre o processo de aquisição, dessa forma os utilizadores estão a par dos resultados. O ciclo do processamento é projectado atendendo aos requisitos estabelecidos de interacção entre a informação armazenada, função de variáveis estabelecidas como por exemplo o tempo. No SIGIC o tempo é um elemento que gera processamentos nos dados registados, criando nova informação e alterando informação já registada, diversos dados podem despoletar transformações nos registos já efectuados de acordo com as metodologias definidas. O ciclo de utilização também se baseia na definição num modelo conceptual. Neste modelo adquire particular importância os aspectos de segurança, os perfis de utilização, a

adaptação às necessidades de utilização, a disponibilidade em tempo e espaço, a ergonomia na sua pesquisa, entre outros aspectos. O objectivo final é utilização pelo utilizador da informação. Os três ciclos são executados indefinidamente.

O modelo de monitorização e controlo da qualidade da informação deve ser construído através da identificação e quantificação dos requisitos da qualidade e definição dos métodos para recolha dos indicadores da qualidade. Em diversos pontos dos ciclos irão existir pontos de controlo onde a informação será avaliada, ou seja, indicadores sobre a qualidade são recolhidos e posteriormente analisados. Consoante os resultados, o processo voltará a um ponto a montante, ponto esse que será determinado pela gravidade das não conformidades detectadas ou a informação é qualificada quanto à sua credibilidade.

Neste processo, pode identificar-se quatro intervenientes:

Intervenientes	Fornecedores (responsáveis por criar ou recolher a informação);
	Utilizadores (consumidores da informação);
	Produtores (responsáveis pelo desenvolvimento, exploração e manutenção dos sistemas e dos dados armazenados);
	Gestores (responsáveis últimos pela informação em todo o processo).

O processo de monitorização da qualidade da informação deve ter conta um conjunto de questões, das quais salientamos as seguintes:

- Os dados registados podem ser interpretados de diversas formas, é imperativo que cada sistema de informação, disponha de um conjunto normalizado de conceitos;
- Um sistema de informação nunca retrata na totalidade o objecto, ter presente os critérios e pressupostos do modelo de aquisição de informação é essencial, na valorização da informação recolhida;
- A informação uma vez arquivada é um recurso que pode ser utilizado indefinidamente, o que levanta problemas no controlo da sua utilização;
- Antecipar o volume da informação a medir, pode ser uma tarefa impossível tal como determinar os pontos óptimos de monitorização;
- Num SI, os utilizadores podem a qualquer momento recorrer à informação existente a aplicá-la de uma forma nunca antes imaginada.

- Os utilizadores que integram a informação, tem de estar inseridos num sistema que garanta o alinhamento motivacional com o relato exacto e actualizado dos objectos a retratar.

- A monitorização tem de estar alinhada com os interesses do negócio no caso da saúde em particular com o interesse dos clientes (utentes e contribuintes).

As técnicas utilizadas ou até mesmo os recursos empregues na resolução dos problemas derivados da qualidade da informação dependem da gravidade que estes assumem nas instituições, logo é preciso adequar as técnicas e os esforços dispendidos aos níveis de qualidade desejados na instituição.

Quando se mede e regista é necessário ter em conta qual a possível utilização da informação, em saúde um pequeno erro de registo pode ter consequências nefastas. A troca de uma identidade pode levar à administração da terapêutica errada a um utente.

É pois importante deixar claro que para falar de qualidade implica assumir inequivocamente as taxas de erro que se consideram aceitáveis, para cada situação, para cada conjunto de informação. Para ser transparente é necessário publicar os objectivos quantificados de qualidade e as análises decorrentes do processo de monitorização.

Existem quatro abordagens complementares para o controlo e garantia da qualidade da informação a saber:

1. Detecção e correcção de erros

Esta técnica tem como alvo a correcção da informação. Consiste em analisar os dados presentes numa base de dados ou nos registos e detectar incorrecções, como valores nulos, informação duplicada ou errada. No entanto, a informação só estará correcta se reflectir a realidade, mas comparar com a realidade milhões de registos é impraticável. Por isso é necessário recorrer à recolha de amostras para posteriormente comparar essas amostras com os valores reais. Esta comparação deverá ter significância estatística e poderá fornecer indicadores sobre a qualidade dos dados presentes na base de dados. A operação de limpeza consiste na correcção da informação errada encontrada. Embora o próprio SI tenha mecanismos de validação da informação, o papel dos utilizadores da informação é importante pois muitas vezes são os responsáveis pela detecção de informação incorrecta.

A origem das incorrecções dos dados pode estar localizada na recolha da informação ou na introdução dos dados no sistema. Alguns erros podem ser evitados com o recurso às seguintes medidas:

- Restrições de domínio e de integridade, presentes na maioria dos sistemas de gestão de bases de dados;

- Sistemas de recolha automática de informação reduzem em muito os erros de digitação;

- A existência de várias ferramentas informáticas que permitem pesquisar volumosas bases de dados para a detecção de possíveis erros, como duplicação de informação, informação inexistente, validação de restrições, valores "anormais, ou tratamento específico de nomes e moradas de utentes.
- No SIGLIC um processo utilizado para promover a detecção e correcção de erros consiste na confrontação de diversos utilizadores com motivações diferentes (profissionais, clínicos, gestores, decisores) com a mesma informação aumentando dessa forma a probabilidade do erro ser detectado
- Outro método utilizado no SIGLIC consiste na determinação dos níveis de consistência e desencadear auditorias aos documentos quando o nível de suspeição é elevado.

2. Análise do processo

Corrigir os erros contidos numa base de dados não é suficiente para assegurar a médio e longo prazo uma base de dados isenta de deficiências. É necessário analisar o processo responsável pela recolha e introdução dos dados e detectar os pontos nos quais os erros são introduzidos, a fim de garantir a prevenção dos erros.

A técnica "*data tracking*" consiste em marcar certos registos de dados no momento da sua recolha e observá-los ao longo do seu percurso. Esta técnica permite observar as alterações que os dados sofrem ao longo do ciclo de vida, para desta forma detectar os pontos nos quais são introduzidos erros ou distorções. Para um processo estabelecido de transformação de informação, é possível colocá-lo sob controlo estatístico, para desta forma observar a evolução dos indicadores da qualidade.

No SIGLIC a informação é analisada face a padrões, face à previsão do normal fluxo dos processos e ainda face a comparadores homólogos. Isso permite identificar situações potencialmente anómalas e desencadear processos de contingência destinados à análise da coerência e eventual correcção dos dados.

Outro processo utilizado no SIGLIC é desencadeado por incidentes que podem consistir em reclamações de utentes ou instituições, na observação de indicadores suspeitos, nas amostragens aleatórias aos dados que determinam o seguimento retrospectivo dos elementos recolhidos para determinação da sua correcção.

3. Metadados da qualidade dos dados

Frequentemente quando um consumidor de informação utiliza um conjunto de tabelas de uma base de dados para pesquisar informação de que necessita, não tem ao seu dispor informação alguma sobre a qualidade dos dados que tem à sua frente. Uma forma de colmatar essa lacuna consiste na inclusão de informação sobre a qualidade desses dados, recorrendo a campos ou a tabelas adicionais.

Por exemplo, informação sobre a data do registo permite avaliar a actualidade dos dados. O número de omissões é utilizado para indicar o número de registos omissos, ou seja, nos quais falta preencher um ou mais atributos. A informação sobre disponibilidade pode dar a indicação do intervalo de tempo entre a recolha da informação sobre um utente e o momento em que a informação é introduzida no SI. Um tempo de disponibilização elevado indica que a base de dados não espelha a actividade real da instituição.

No SIGLIC a informação é qualificada no seu desvio face aos padrões e limitadores estabelecidos e face aos históricos de ocorrência. A título de exemplo o registo dum novo utente identificado com uma data de nascimento anterior a 1880, sem data de nascimento, com data nascimento superior a data do registo é classificado como errado, a variação do número de registos de cirurgias em mais de 100% num período de 3 meses é classificado como um potencial erro; uma média de tempo de espera 2 vezes superior ao padrão é classificada como um potencial erro e desencadeia um processo de averiguações.

4. Gestão da qualidade total

O “total quality management” (TQM) representa a abordagem mais organizacional ao problema da gestão da qualidade. É antes de mais uma filosofia ou atitude baseada no princípio da melhoria contínua, na crença de que é sempre possível fazer mais e melhor. É uma abordagem disciplinada que integra técnicas de gestão com ferramentas da qualidade.

A actuação da gestão da qualidade total está centrada no ciclo de melhoria contínua para a qualidade da informação:

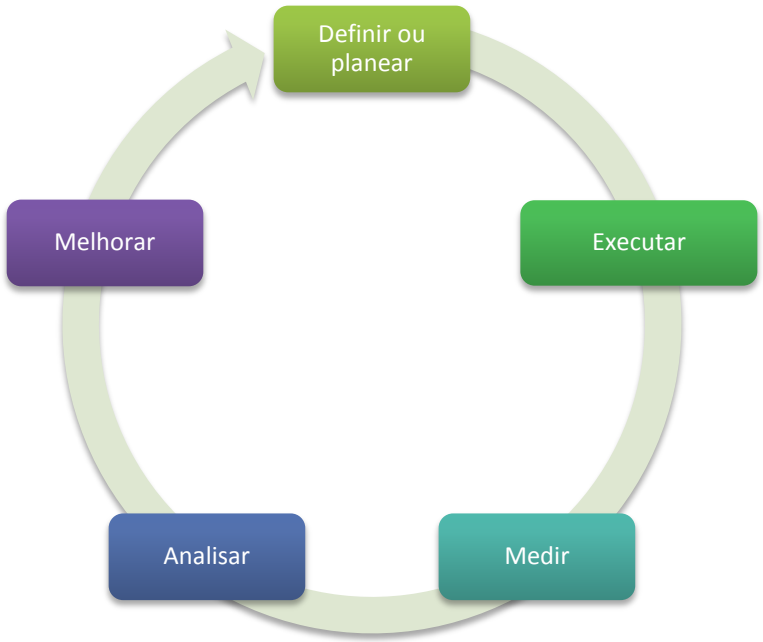


Ilustração 8: Ciclo de melhoria contínua para a qualidade da informação

Este ciclo consiste em planear estabelecendo objectivos, executar o plano, recolher medidas de desempenho actual de acordo com os indicadores definidos, comparar os indicadores de desempenho com os objectivos traçados e actuar, alterando/melhorando o processo para diminuir a diferença de resultados obtida.

No SIGIC utiliza-se esta metodologia em dois níveis de processos paralelos: um avaliando a produção de resultados conformes com os objectivos estabelecidos e promovendo a melhoria contínua dos processos; Outro avaliando os objectivos estabelecidos em função dos princípios enunciados função das respostas obtidas promovendo uma melhoria contínua dos objectivos.

Esta abordagem assenta em três pilares básicos: a informação, o ciclo de melhoria contínua e a gestão do processo. A informação deve ser descrita, realizando para tal a identificação das suas características e dos seus requisitos de qualidade, e a definição do sistema que irá produzir a informação.

Ao designar a informação como um recurso e ao atribuir-lhe os recursos necessários para que a informação consumida tenha as características adequadas à sua utilização, ou seja, tenha qualidade, estamos a criar um sistema de garantia da qualidade da informação. Tal sistema deverá assegurar que a função qualidade está alinhada com a estratégia da instituição hospitalar, está instalada e que obtém os resultados pretendidos.

A necessidade de gerir a qualidade da informação surge com a complexificação progressiva dos sistemas e decorre essencialmente da necessidade de ser eficiente e operar num contexto de risco controlado. No negócio da saúde a informação não é só um meio

instrumental é também um produto final em si mesmo. Nesta medida a necessidade de qualidade está também directamente correlacionada com o valor do serviço prestado e consequentemente com a sustentabilidade do próprio negócio. Outra vertente da mesma realidade prende-se com os custos, isto é se pretendermos controlar valor e risco para garantir a sustentabilidade do negócio e não possuirmos informação com qualidade os custos associados ao negócio serão necessariamente superiores, pois não saberemos onde cortar desperdícios sem afectar o valor.

A gestão da qualidade dos dados envolve a especificação de políticas, a identificação de técnicas e a utilização de procedimentos para assegurar que os dados da instituição possuem o nível de qualidade adequado para a sua utilização actual e futura. Na área da saúde esta decisão deve ser promovida pela tutela, acarinhada por sociedades científicas, acompanhada pelo compromisso da gestão ao mais alto nível da gestão da unidade de saúde. As administrações devem ser julgadas pela qualidade da informação produzida nas suas instituições. A criação de uma cultura de transparência e qualidade assim como o fomento da comunicação entre os departamentos e entre colaboradores são requisitos básicos na promoção de um sistema de informação sustentável.

Medir a qualidade é identificar quantificar e contextualizar os desvios. Estes serão analisados e qualificados de positivos ou negativos. Quando negativos as acções visão identificar e corrigir as razões subjacentes, quando positivos a acção corresponde á reformulação do modelo.

O sistema de informação numa unidade de saúde deve contemplar a existência de um gabinete/departamento de gestão de informação que contenha gestores das diversas especialidades de informação geridas pelo sistema. Assim sendo o “cor Business” do negócio a saúde, um clínico tem de estar envolvido ao mais alto nível na gestão da informação. Não obstante, um envolvimento directo de um delegado da administração, de um gestor de qualidade, de um colaborador com competência em estatística e de um informático é fundamental para o sucesso deste organismo.

O modelo de garantia da qualidade da informação tem como objectivo assegurar que todas as actividades ou processos que, de alguma forma, podem influenciar a qualidade da informação estão identificados e controlados, assim como antecipar as necessidades actuais e futuras de informação na instituição.

As responsabilidades atribuídas ao departamento de gestão de informação são, entre outras:

- Perscrutar e reconhecer a natureza da informação e a importância desta no negócio;
- Definir, planear e implementar os processos de gestão da informação;
- Definir, planear e implementar as políticas que asseguram a qualidade da informação;

- Encontrar o ponto de equilíbrio entre requisitos ou necessidades contraditórios;
- Gerir a relação custo benefício da qualidade da informação;
- Promover na instituição uma cultura de qualidade e transparência;
- Promover programas de sensibilização e formação no que se refere aos sistemas de informação tendentes à garantia da qualidade de informação;
- Gerir o risco associado à utilização da informação, estabelecendo sistemas de monitorização, protocolos e planos de contingência;
- Reportar periodicamente resultados (desvio dos indicadores aos objectivos estabelecidos), nível de risco e constrangimentos;
- Reportar inequivocamente à gestão de topo, todas as situações que podendo comprometer o sistema ultrapassem o departamento na sua capacidade de controlo;
- Propor, decorrente da análise dos relatórios produzidos pela monitorização, alterações aos modelos iniciais, numa lógica de melhoria contínua.

Em seguida enuncia-se um conjunto mínimo de actividades associadas à garantia da qualidade da informação são as seguintes:

- **Manutenção de um inventário do recurso informação**

Que dados existem numa organização, quem e quando os produz, quem e com que finalidade os consome, são perguntas a que um inventário deverá responder. À semelhança de outros recursos, a instituição hospitalar precisa de saber o que está ao seu dispor em termos do recurso informação. Trata-se da constituição de um inventário, através da modelação de dados ou diagramas de fluxo. Neste processo é necessário inquirir todos os serviços, levantar todos os processos formais e informais. É também uma boa oportunidade para formalizar processos informais e rever os já instituídos.

- **Criação do suporte normativo**

Cabe aos gestores da qualidade da informação propor o conjunto de políticas, procedimentos e de normas que considerem necessários para o bom desempenho do sistema de garantia da qualidade da informação. Estes devem ser, pela administração, validados face aos princípios institucionais e à missão estabelecida e em seguida veementemente implementados. Por exemplo, devem ser estabelecidas políticas e normas para questões como o acesso à informação, segurança dos dados, métodos para recolha de informação, instrumentos de

recolha e análise de informação, processos de migração, definição de requisitos de informação, entre outros.

- **Identificação e correcção de deficiências**

O modelo de garantia da qualidade deve criar condições para que as deficiências identificadas em qualquer ponto do processo dêem origem a medidas correctivas a fim de evitar a reincidência do defeito. A identificação de deficiências deve constituir oportunidades em medidas de melhoria na eficácia e na produtividade. Neste ponto temos de garantir a existência de planos de contingência adequados.

- **Formação**

À função qualidade são atribuídas responsabilidades na área da formação e da sensibilização a todos os colaboradores que de alguma forma se encontram envolvidos em actividades que podem afectar a qualidade da informação, sejam eles parte do grupo dos fornecedores, consumidores, produtores ou dos gestores, adequando os colaboradores à função ou tarefa que executam, dotando-as dos conhecimentos e das técnicas mais apropriados.

As acções de formação têm de ser credibilizadas pela avaliação dos conhecimentos apreendidos. Outro aspecto é o de determinar o impacto nos processos e na organização decorrente da formação.

Uma formação para a mudança tem de ser concomitantemente completada pela *desfuncionalização* do processo anterior, a monitorização da *compliance* com o novo processo e instituição de um modelo de incentivos e penalizações.

- **Lançamento e o controlo de projectos de melhoria**

A qualidade não é só da responsabilidade do departamento da qualidade mas de todos no seio da organização. Se é reconhecida a competência nos indivíduos envolvidos, então estes constituem uma fonte de inovação e de informação não negligenciável para a melhoria contínua, pelo que é necessário envolvê-los activamente na procura das melhores soluções. É da responsabilidade da função qualidade criar condições para que os colaboradores da instituição tenham uma atitude participativa, por exemplo através de equipas voluntárias, dando-lhes os recursos necessários, e que as suas propostas tenham um encaminhamento apropriado, quer sejam aceites ou rejeitadas, sendo o seu trabalho seja observado e controlado para garantir a compatibilidade organizacional.

As instituições hospitalares são organizações em que o conhecimento técnico dos colaboradores que a compõem é o seu capital mais valioso. Cabe aos gestores da informação captar este capital, geri-lo e potencia-lo.

Quer seja de uma forma espontânea ou programada, cabe à função qualidade a identificação dos projectos de melhoria, a realização de análises custo-benefício das diversas propostas, a calendarização da acções, o controlo da execução das acções e a análise de resultados.

- **Controlo do desenvolvimento de produtos de informação.**

Os consumidores não querem SI, mas sim informação com qualidade. Um SI é concebido e construído com o propósito de fornecer informação com qualidade aos seus utilizadores.

Por vezes a actividade de desenvolvimento de um SI não produz os resultados esperados devido à não satisfação dos requisitos de qualidade da informação dos utilizadores. Esta abordagem levanta vários problemas nomeadamente:

- A falta do levantamento inicial das características desejadas para a informação antes da análise do processo de aquisição e armazenamento dos dados;
- A maioria dos *inputs*, sejam eles formulários ou informação electrónica, não são adequados, pois não servem as necessidades operacionais. Apresentam incorrecções, lacunas e são frequentemente utilizados de outras formas que não as inicialmente planeadas;
- O armazenamento de dados, nomeadamente o modelo conceptual, está muito mais vocacionado para as necessidades de aquisição do que as de extracção;
- A utilização de informação surge aparentemente como assegurada, pois apenas corresponde a diferentes combinações dos dados recolhidos;
- É recolhida e armazenada informação que não tem qualquer utilidade;
- A questão da qualidade resume-se à definição de um conjunto de restrições aplicadas como filtros na entrada dos dados e à responsabilização do utilizador, aqui no papel de fornecedor, por toda a informação que escapou às restrições colocadas. A responsabilidade pela má qualidade dos dados parece repartida entre produtores e fornecedores.

O desenvolvimento de um produto de informação começa pela definição das características desse produto e dos seus requisitos de qualidade. Esta definição não é estática e tem de evoluir em contínuo tal como evolui o negócio e sua envolvente. A exigência aos serviços é cada vez maior, fruto da competição entre prestadores que procuram cada vez mais

aproximar-se dos anseios dos consumidores e dessa forma conquista-los. A consequência directa é uma necessidade de uma maior qualidade nos sistemas de informação.

Depois de definido o produto, passa-se à avaliação do estado do recurso informação para ver se o produto pretendido pode ser disponibilizado. Numa primeira instância, pode ser apenas necessário definir o ciclo de utilização de informação, que consiste, como já foi dito anteriormente, na definição do conjunto de dados necessários, na construção dessa "*view*", e na extracção e posterior apresentação da informação. Se tal não for possível, será então necessário construir todo o caminho que se inicia nas fontes de informação, passa pela construção do ciclo de aquisição de dados, armazenamento e o posterior ciclo de utilização.

Para que a qualidade da informação seja salvaguardada é necessário que as actividades de desenvolvimento de um SI sejam capazes de traduzir os requisitos de informação dos utilizadores em sistemas capazes de os satisfazer.

Os gestores da informação devem ser detentores da visão do estado actual da informação mas também de uma visão estratégica, de uma visão que aponte os caminhos a seguir para que a informação preste o papel mais útil à organização, permitindo a própria evolução desta última. Partirá da função qualidade a iniciativa de fomentar junto da organização novas utilizações para a informação. Quanto mais informação for utilizada, maior será a qualidade desta e maior será o efeito positivo na organização.

O utilizador é o único elemento capaz de identificar desvios entre a informação que recebe do SI e a sua contrapartida no mundo real. Quanto mais intensiva for a utilização da informação, maior número de não conformidades serão detectadas. Assim existem um conjunto de regras para a qualidade da informação:

- Dados não utilizados dificilmente podem ser qualificados quanto à sua correcção;
- A qualidade da informação deve ser primariamente determinada em função do seu uso e não da sua recolha e armazenamento, não obstante atendendo à possibilidade de utilizações não antecipáveis a recolha e armazenamento devem garantir uma qualidade suficiente à generalidade das potenciais utilizações;
- A qualidade dos dados não será superior à correspondente à sua utilização mais intensiva e está condicionada à etapa mais crítica de todo o processamento;
- Os problemas com a qualidade da informação tendem a agravar-se à medida que o sistema envelhece, se este não se for transformando de forma a acompanhar a evolução do negócio;
- Quanto menor for a frequência de actualização de um dado elemento, mais drástica é essa mudança;
- As leis da qualidade da informação aplicam-se aos dados e aos metadados.

Existem vários mecanismos para garantir a qualidade da informação nos SI, dos quais salientamos os seguintes:

- Implementação dos requisitos de normas internacionais nas valências da informática de gestão, ao nível funcional / departamental e/ou de software;
- Elaboração de procedimentos e outros documentos da qualidade (formalização dos sistemas) orientados para certificação;
- Elaboração de auditorias SI/TI (preparação e elaboração do relatório de auditoria, técnicas de execução), realização de inspecções (qualidade do software) e controlo interno (gestão de recursos SI/TI organizacionais);
- Gestão e planeamento da qualidade em projectos TIC;
- Utilização de *software* para gestão da qualidade da informação.

4.2. Segurança em SI

4.2.1. Considerações gerais sobre segurança da informação

A segurança dos SI é um dos elementos incontornável na utilização da informação nas instituições, uma vez que:

- Minimiza os prejuízos da instituição decorrentes da indisponibilidade da informação;
- Garante a qualidade dos dados inseridos e das informações geradas;
- Garante a sustentabilidade dos dados ao longo do tempo;
- Impede o roubo ou a utilização não autorizada dos dados;
- Evita ataques externos pela rede intranet / internet.

A segurança em SI está intrinsecamente ligada à segurança da informação, que não é mais do que a protecção dos dados no sentido de preservar o valor que possuem para os utilizadores e para a instituição. Assim, a segurança em SI abrange todos os aspectos relacionados com a protecção de informação e dos dados e da protecção dos SI em si.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da segurança existente. A segurança de uma determinada informação pode ser afectada por factores comportamentais e de uso negligente por parte dos utilizadores ou por parte de pessoas mal-intencionadas que têm o objectivo de roubar, destruir ou modificar essa informação. A segurança também pode estar comprometida por falhas técnicas,

acidentes e catástrofes. A segurança da informação permite, por um lado, a protecção da informação e dados contra a sua destruição, deterioração, modificação não autorizada, intencional ou acidental, e previne, por outro, o mau uso dos recursos informáticos, nomeadamente a protecção dos computadores contra danos e uso não autorizado e a protecção dos SI de modificações não autorizadas.

A segurança da informação compreende um conjunto de medidas que visam proteger e preservar informações e sistemas de informações, assegurando-lhes os seguintes atributos:

- **Confidencialidade**: limitar o acesso da informação somente aos utilizadores autorizados (prevenção do acesso não autorizado a informações, além de manter dados e recursos ocultos a utilizadores sem privilégio de acesso);
- **Integridade**: prevenir a modificação não autorizada de informações a par da garantia de que a informação manipulada mantém as características originais, através de um sistema de versões que constitui o controlo de alterações e garante a identificação dos seus autores localizando-os no tempo na conjuntura;
- **Disponibilidade**: garantir um acesso confiável e prontamente disponível à informação por parte dos utilizadores (a informação deve estar sempre disponível para uso pelos utilizadores autorizados) no espaço, tempo e forma apropriados à sua utilização;
- **Autenticidade**: garantir que o SI tem condições para verificar a identidade e autenticidade dos utilizadores, e os utilizadores têm condições de analisar a identidade do SI;
- **Não-repúdio ou irretratabilidade**: não deverá ser possível ao autor da informação negar a autoria da mesma;

Estes elementos constituem os cinco pilares da segurança da informação e, portanto, são essenciais para assegurar a integridade e confiança nos sistemas de informações. Devem assim orientar a análise, o planeamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger.

O nível de segurança desejado deve traduzir-se numa política de segurança que é seguida pela instituição, de forma a garantir que uma vez estabelecidos os princípios, aquele nível desejado seja alcançado e mantido. Para criar esta política, deve-se ter em conta:

- Riscos associados à falta de segurança;
- Benefícios decorrentes da segurança da informação;
- Custos de implementação dos mecanismos.

O nível de segurança deve ser estabelecido individualmente em função de cada um dos 5 pilares, pois consoante a utilização uns podem ser mais importantes que outros.

A segurança da informação correlaciona-se directamente com a confiança que nela depositamos.

Um aspecto a ter em conta é que a segurança da informação é apenas um componente da segurança do negócio. A título de exemplo, se confiarmos pouco num determinado sistema que regista a prescrição terapêutica, para garantirmos a segurança do negócio colocamos sistemas redundantes tais como, por exemplo, vários interlocutores que confirmam a prescrição, podendo bloquear em diversos momentos a administração da terapêutica. Importa pois nestes casos determinar os custos alternativos à segurança da informação.

4.2.2. Ameaças à segurança

As ameaças à segurança da informação são relacionadas directamente com a perda de um ou mais atributos, nomeadamente a perda de confidencialidade (ex.: quebra de sigilo da senha de um utilizador ou administrador de sistema), a perda de integridade (a informação fica exposta para manipulação por elementos não autorizados) e a perda de disponibilidade (ex.: perda de comunicação com o SI, que aconteceu com a avaria de um servidor ou a falha de uma aplicação crítica da instituição).

Os principais problemas causados pela falta de segurança nos SI são a corrupção ou perda de dados e as invasões de intrusos. A perda de dados e as ameaças à rede informática ou aos SI na maioria das vezes é causada por:

- Factores naturais (incêndios, inundações, terramotos, etc.);
- Falhas na infra-estrutura operacional (falta de energia, queda de comunicações, falhas de equipamentos, má utilização e erros de hardware ou de software, falhas no

processamento, erros de comunicação, erros de configuração, *bugs* em aplicações, etc.);

- Erros humanos (entrada de dados incorrecta, montagem errada do disco ou perda de um disco);
- Sobre utilização das infra-estruturas de forma não programada ou negligenciada
- Agentes maliciosos e invasores (*hackers*, *crackers*, vírus, utilizadores mal treinados, funcionários descontentes, etc.).

Os pontos mais vulneráveis na estrutura de tecnologias de informação são:

- Redes de comunicação;
- Sistemas operacionais dos equipamentos;
- Bases de dados e aplicações;
- Servidores;
- Acesso à internet.

4.2.3. Políticas e mecanismos de segurança

Para lidar com as ameaças à segurança, torna-se necessário a definição de políticas e mecanismos de segurança, visando dar suporte a:

- Prevenção – evitar que invasores violem os mecanismos de segurança;
- Detecção – habilidade de detectar invasão aos mecanismos de segurança;
- Recuperação – mecanismo para interromper a ameaça, avaliar e reparar danos, além de manter a operacionalidade do sistema caso ocorra invasão ao sistema.

Uma política de segurança de informação e dos SI consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos informáticos de uma instituição.

As políticas de segurança devem ter em conta as normas internacionais, ter implementação realista, e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da gestão de topo. Deve também adaptar-se a alterações na instituição. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

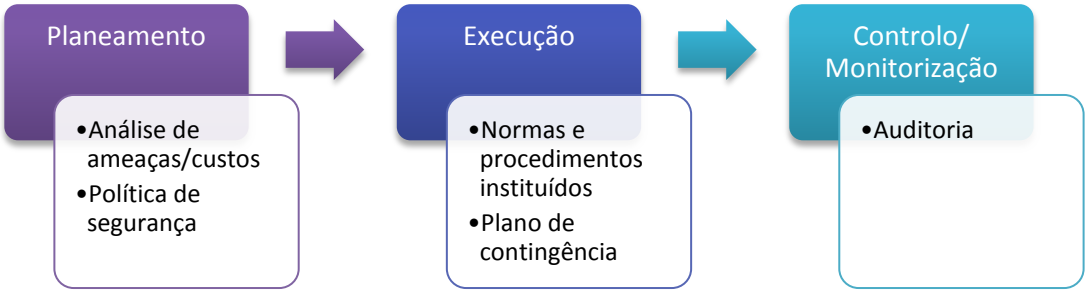
O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

A política de segurança deve ter em conta os atributos para a segurança da informação, nomeadamente a disponibilidade, a integridade, a autenticidade, a confidencialidade e ainda a utilização (o SI deve ser utilizado para os objectivos determinados para o mesmo).

No âmbito da definição das políticas e mecanismos de segurança, a instituição têm que decidir o nível de segurança a estabelecer para uma rede ou sistema. No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de protecção para minimizar a probabilidade de ocorrência de um ataque.

Existem 3 níveis de segurança da informação:

- **Segurança operacional**: impõe barreiras às ameaças ao ciclo de gestão da segurança na instituição, sendo o seguinte:



- **Segurança física**: impõe barreiras às ameaças físicas limitando o contacto ou acesso directo à informação ou à infra-estrutura que a suporta, tais como catástrofes naturais (incêndios, terramotos, relâmpagos, inundações), acesso indevido de pessoas, forma inadequada de tratamento e utilização do SI e respectivas infra-estruturas;

> Por exemplo, portas, trancas, paredes, blindagem, seguranças, etc.

- **Segurança lógica**: barreiras que impedem ou limitam o acesso à informação contra ameaças à integridade, autenticação e privacidade do SI e causadas por ataques como vírus, acessos remotos à rede, backups desactualizados, violação de senhas, erros não intencionais (ex.: remoção acidental de arquivos de sistema ou aplicação), etc.

Por exemplo, criptografia (permite a transformação reversível da informação de forma a torná-la ininteligível a terceiros, através de algoritmos e chaves secretas), assinatura digital (dados criptografados associados a um documento), controlo do acesso (através de palavras-chave, sistemas biométricos, *firewalls*, cartões inteligentes, etc.), certificação de documentos, protecção contra personificação por intrusos, *softwares* para detecção e eliminação da acção de *crackers*, *hackers*, *spammers*, vírus e outros agentes externos intrusos no SI, protocolos de segurança, etc.

4.2.4. Medidas de segurança

As medidas de segurança nos SI visam proteger os computadores contra danos e uso não autorizado e os programas e dados de modificações não autorizadas.

Para garantir a protecção e segurança dos SI e da informação, é necessário adoptar as seguintes medidas agrupadas em 3 grandes grupos:

- Gerais:
  - Auditoria aos sistemas de segurança implementados
  - Cópias de segurança (Backups) regulares e sistemáticos, guardados longe dos dados originais (é habitual a realização de backup total semanal e backups diários incrementais);
  - Redundância nos registos com arquivo em locais separados territorialmente (de preferência regiões distintas do país para prevenir que uma catástrofe elimine todas as cópias dos dados;
  - Replicação de registos em sistemas de distintos fabricantes (reforçando a garantia de um acesso independente aos dados);
  - Sistema para protecção de arquivos (conjunto de regras que garantem que a informação não seja lida, ou modificada por quem não tem permissão).
- De autenticação dos utilizadores: obrigatoriedade de identificação do utilizador no computador ou SI através de usuário e senha (password), que devido ao seu carácter pessoal e intransmissível, serve para autenticar o utilizador (verificar a sua identidade) e determinar os seus privilégios de acesso. De preferência a identificação do utilizador deve ser estabelecida por dois métodos concomitantes um decorrente de parâmetros biométrico

(impressão digital, imagem da retina, …) outro do tipo *password* digitado ou identificação por cartão, chave de acesso.

Uma boa senha deve ter pelo menos oito caracteres (letras, números e símbolos), deve ser simples de digitar e, o mais importante, deve ser fácil de lembrar, deve ainda ser alterada periodicamente e não replicada em diversos sistemas.

Apresentam-se alguns exemplos de normas de senhas de acesso ao SI de forma a prevenir o seu mau uso por parte dos utilizadores:

- Senha com data de expiração: a senha possui prazo de validade com 30 ou 45 dias, obrigando o colaborador ou usuário a renovar sua senha;
- Inibir a repetição: uma senha uma vez utilizada não poderá ter mais que 60% dos caracteres repetidos;
- Obrigar a composição com número mínimo de caracteres numéricos e alfabéticos (por exemplo, define-se a obrigatoriedade de 4 caracteres alfabéticos e 4 caracteres numéricos na senha);
- Criar uma base de dados com formatos conhecidos de senhas que não podem ser utilizadas (por exemplo o utilizador chama-se Jose da Silva, logo sua senha não deve conter partes do nome como 1221jose, os formatos DDMMAAAA, etc.);
- Utilizar senhas com *Case Sensitive* e caracteres especiais como: @ # $ % & *.

- Controlo do acesso: utilização de dispositivos de *hardware* e *software* bem instalados e configurados que permitem o que pode ou não passar no perímetro interno de comunicação da instituição;

Por exemplo, *routers*, *firewalls* para proteger a comunicação entre 2 ou mais redes, software de remoção de agentes intrusos e de ataques como vírus, *crackers*, *spammers*, VPN (Virtual Private Network) que permite proteger o canal de comunicação entre dois computadores distantes, a manutenção de *logs* que permitem investigar uma invasão na rede interna, software de monitorização da segurança na rede interna para descobrir falhas de configuração local das estações de trabalho e as alterações a fazer para proteger o SI, controlar o acesso dos utilizadores à internet, etc.;

- Criptografia: sistemas de encriptação de dados que servem para autenticar a identidade de utilizadores, autenticar e proteger o sigilo de comunicações, informações e transacções electrónicas e proteger a integridade da informação, através da codificação dos dados entre os utilizadores e o SI;

Os sistemas de certificação podem ser de chaves ou de certificados. Nos sistemas de chaves a informação só é acessível com a chave. Nos sistemas certificados verifica-se a autenticidade do emissor e receptor da informação de modo a garantir a sua integridade (ex.: certificados digitais certificam a identidade de um documento electrónico).

- De disponibilidade: existência de infra-estrutura de redundância (exemplo, servidores e base de dados redundantes);
- Protocolos de segurança;

Por exemplo, o protocolo SSL (Secure Sockets Layer) desenvolvido pela Netscape permite a privacidade e a integridade de dados entre duas aplicações que estejam a comunicar entre si pela Internet, através da autenticação das partes envolvidas e da criptografia dos dados transmitidos entre as partes. Esse protocolo ajuda a prevenir que intermediários entre as duas pontas da comunicação tenham acesso indevido ou falsifiquem os dados que estão a ser transmitidos.

O protocolo TLS (Transport Layer Security) é um protocolo de segurança de rede usado para criptografar e transmitir dados HTTP e IPP (Internet Printing Protocol) por uma rede TCP/IP. Ele é baseado e similar ao protocolo SSL.

O protocolo PGP (Pretty Good Privacy) utiliza a encriptação para proteger o correio electrónico e arquivos de dados, garantindo a sua privacidade e autenticação.

Quer as políticas quer as medidas devem ser comunicadas amplamente na organização, a adesão dos colaboradores deve ser medida. Também devem ser periodicamente testadas no sentido de determinar potenciais falhas. Outro aspecto importante é a efectivação de simulacros para treinar os participantes e testas os processos de contingência.