Sistemas de Informação na Saúde

2º Parte

Agenda

- Responsabilidade (cont.)

- RGP: Objetivos e Lista de Conformidades

- Privacidade de Dados de Saúde

- Princípios base de proteção de dados no contexto da saúde

- Bases Legais para o Tratamento de Dados

Agenda

- Transparência

- Direitos dos Titulares de dados

- Ameaças de Segurança

- Políticas de Proteção de Dados

- Disponibilidade: Políticas de Backups e Disaster Recovery (DR)

- Processo de Gestão da Segurança da Informação: Políticas de Segurança

Responsabilidade

adaptado de: Hospital de Braga

Desafio

Quais são os intervenientes responsáveis pela proteção e segurança dos dados de saúde?

Responsabilidade

Intervenientes:

- CA - Conselhos de Administração
- SI - Serviços de Sistemas de Informação
- DPO – Encarregado de Proteção de Dados
- CISO – Chief Information Security Officer
- Transversais (utente)

Responsabilidades Transversais

Quem deve definir os perfis de Acesso às aplicações?

As Direções e Serviços!

Serviço de Sistemas de Informação deve apenas ser informado dos perfis de acesso definidos.

Selecionar Entidades Externas que sigam políticas e regulamentos!

É da responsabilidade dos serviços que selecionam entidades externas garantir o respeito pela política e regulamentos instituídos!

Responsabilidade Transversais

Comunicação de Responsabilidades!

Colaboradores devem saber das suas responsabilidades, em matéria de Segurança da Informação, tais como:

- confidencialidade da informação,
- utilização dos sistemas de informação de acordo com as políticas e regulamentos definidos,
- código de conduta/ética aplicável, entre outros.

Responsabilidade Transversais

Todos os colaboradores devem ser responsáveis pelo cumprimento das políticas e regulamentos de Segurança da Informação em vigor!

Cumprimento de cláusulas de confidencialidade, utilização adequada e responsável dos equipamentos informáticos e documentos físicos, zelar pela segurança dos ativos do Hospital e comunicar qualquer incidente de Segurança da Informação identificado.

Desafio

Será fácil toda esta articulação e gestão??

RGPD

RGPD – Objetivos Macro

https://www.youtube.com/watch?v=Assdm6fIHlE

- Educar os utilizadores sobre os seus processos de recolha e tratamento de dados.

- Notificar os utilizadores sobre as razões do tratamento dos seus dados.

- Obter autorização prévia para tratar os dados dos utilizadores.

- Tornar anónimos os registos recolhidos.

RGPD – Objetivos Macro

- Permitir aos utilizadores retirar o seu consentimento para o processamento de dados.

- Notificar os utilizadores de quaisquer violações.

- Dar aos utilizadores acesso aos registos.

- Assegurar transferências de dados seguras através das fronteiras.

- Eliminar informações mediante pedido.

RGP – Lista de conformidade

- A entidade tem um responsável pela proteção de dados?
- Está definido um processo para rever os dados recolhidos?
- A sua política de privacidade foi elaborada pelo DPO?
- Os utentes estão conscientes de como a sua informação será utilizada e porque é que é necessária?
- Existe um período de retenção adequado para a recolha de quaisquer dados?
- Teve alguma violação de dados nos últimos 18 meses? Em caso afirmativo, estas foram comunicadas ao DPO no prazo de 72 horas após a sua descoberta, conforme exigido pelo RGPD.

Privacidade de dados de saúde

Privacidade

Garante o direito de limitar quem acede a informação pessoal.

Restrição de Acessos

Um sub-requisito mais complexo, para alguns pacientes, é permitir o **acesso distinto e diferencial** a partes do seu registo de saúde. Por exemplo, direitos de acesso relativamente abertos à maior parte do registo de saúde, mas acesso limitado a itens de saúde sexual ou mental.

A **inter-relação** da informação de saúde pode tornar isto bastante complexo.

Por exemplo, a lista de medicamentos irá muitas vezes dar condições sensíveis mesmo que o diagnóstico esteja oculto, mas é necessário para qualquer tratamento seguro, e muitos profissionais de saúde considerariam a indisponibilidade da informação atual sobre medicamentos e alergias como altamente problemática para dar mesmo cuidados básicos.

Princípios base de proteção de dados no contexto da saúde

adaptado de: WHO

Princípios base de proteção de dados

Para assegurar o pleno cumprimento das leis e regulamentos aplicáveis à proteção de dados, naturais ou legais as pessoas que processam dados pessoais devem aderir aos seguintes princípios de proteção de dados.

Justo, lícito e transparente

os dados pessoais devem ser tratados de forma justa, lícita e em de forma transparente em relação à pessoa a quem os dados dizem respeito. Em particular, os dados pessoais devem não ser processado, salvo se permitido por lei, com base num interesse legal preponderante da processador ou consentido pelo sujeito dos dados.

Limitação da finalidade

os dados pessoais devem ser obtidos apenas para um ou mais especificados e fins lícitos, e não devem ser posteriormente processados de forma incompatível com esse objetivo ou esses objetivos.

Princípios base de proteção de dados

Exatidão

Os dados pessoais devem ser exatos e, se necessário, mantidos atualizados.

Minimização dos dados

Os dados pessoais devem ser adequados, relevantes e limitados ao que é necessário em relação ao fim para o qual são processados.

Limitação de armazenamento

os dados pessoais tratados para quaisquer fins não devem ser conservados por mais tempo do que é necessário para esses fins.

Princípios base de proteção de dados

Direitos das pessoas em causa

os dados pessoais devem ser tratados de acordo com os direitos de pessoas em causa, tal como estipulado pelas leis de proteção de dados aplicáveis.

Integridade e confidencialidade

Física, técnica, legal e organizacional. Devem ser tomadas medidas contra o tratamento não autorizado ou ilegal de dados pessoais e contra perda acidental, alteração ou dano de dados pessoais.

(Open EHR)

Princípios base de proteção de dados

Transferência internacional de dados pessoais

Os dados pessoais não serão transferidos para um terceiro país ou organização internacional, a menos que esse país/organização assegure um nível de proteção dos direitos e liberdades das pessoas em causa em relação ao tratamento de dados pessoais.

(utilização de HL7-FHIR)

Bases legais para o tratamento de dados

adaptado de: WHO

Bases Legais

Independentemente da finalidade do tratamento de dados pessoais, esse tratamento não é, prima facie permitido, a menos que o responsável pelo tratamento de dados tenha uma base legal válida para o fazer (artigo 6º da GDPR).

Bases Legais

Estão disponíveis seis bases legais para o tratamento de dados:

- Não há uma melhor ou mais importante do que as outras.
- O que é mais apropriado para usar depende do objetivo do processamento e da relação com o indivíduo.

A base legal deve ser determinada **antes** do **processamento**, e deve ser devidamente documentado, de acordo com o processamento atividade.

Bases Legais

Consentimento

O titular dos dados deu um claro consentimento informado para o tratamento de dados pessoais dados para um fim específico.

(HL7 FHIR/Security and Privacy/Consent)

Contrato

O tratamento dos dados é necessário para executar um contrato que o responsável pelo tratamento de dados tem com o individuo, ou porque a pessoa em causa pediu que fossem tomadas medidas antes de entrar em vigor um contrato.

Bases Legais

Obrigação legal

O processamento de dados é necessário para o cumprimento da lei (não incluindo obrigações contratuais).

Interesses vitais

O processamento de dados é necessário para proteger a vida de alguém.

Tarefa pública

O processamento de dados é necessário para o desempenho de uma tarefa de interesse público ou como parte de uma tarefa ou função oficial, e a tarefa ou função tem uma base clara na lei.

Bases Legais

Interesses legítimos

O processamento de dados é necessário para o interesse legítimo de terceiros, a menos que haja uma boa razão para proteger os dados pessoais do indivíduo, o que prevalece sobre os interesses legítimos.

Esta base jurídica não se aplica se uma autoridade pública está a processar dados pessoais a fim de desempenhar as suas tarefas oficiais.

Bases Legais

A instituição deve:

- Desenvolver uma compreensão holística dos princípios.

- Desenvolver um plano sobre como operacionalizar os princípios no contexto específico.

- Desenvolver um plano a longo prazo sobre como aderir a estes princípios de forma sistemática.

Bases Legais

A instituição deve:

- Definir a base jurídica específica para o processamento de dados.

- Considerar cuidadosamente a utilização do consentimento informado como base jurídica.

- Utilizar a base de interesse vital apenas em casos excecionais, se a intervenção de saúde pública for o benefício direto dos sujeitos dos dados.

- Documentar todas as deliberações e quaisquer decisões tomadas adequadamente.

Bases Legais – Consentimento Informado

O consentimento informado não é um "atalho”

- Avaliar cuidadosamente se esta é a ferramenta certa para a situação de processamento de dados.

- Avaliar cuidadosamente o grau de liberdade da pessoa a quem os dados se destinam.

- Comunicar claramente à pessoa em causa que esta tem, de facto, uma escolha.

- Ser granuloso e específico: evitar consentimentos amplos ou genéricos, se possível.

Bases Legais – Consentimento Informado

CONSENTIMENTO:

O Quê? Quem? Como? Quando? E para quê?

- Âmbito
- Tipo Informação
- Duração
- Identificação do destinatário
- Objetivo da informação

Entidade Reguladora da Saúde

Transparência

adaptado de: WHO

Transparência

A instituição deve:

- Desenvolver uma política de privacidade e publicar a política no website ou através de outros meios.

- Certificar que utiliza uma linguagem simples e acessível.

- Certificar de que dispõe de canais de comunicação que permitem o fácil acesso.

- Trabalhar proactivamente com a sociedade civil para comunicar os seus conceitos de proteção de dados e processos.

Direitos dos titulares de dados

adaptado de: WHO

Direitos dos Titulares de Dados

Direito de acesso

a) o direito de saber se os dados relativos estão a ser processados.

b) em caso afirmativo, o direito de aceder a esses dados e de obter uma cópia de os dados.

Direito à retificação

Significa que, quando os dados pessoais estão incorretos, as pessoas em causa podem exigem que os controladores corrijam dados factualmente incorretos.

Direitos dos Titulares de Dados

Direito ao esquecimento

Em algumas situações nomeou-se o direito a ser esquecido, caso os dados pessoais tenham sido tornados públicos.

É um direito fundamental para restringir o processamento de dados e para impor períodos de retenção.

Direito à restrição do processamento

Direito de um cidadão a limitar os tratamento dos seus dados pessoais, se puderem reivindicar um direito preponderante de restringir o processamento.

Direitos dos Titulares de Dados

Direito a ser informado

Deve ser entendido como a pedra angular dos direitos da pessoa em causa. A maior parte das leis de proteção de dados na Europa e noutros locais obrigam aos responsáveis pelo tratamento informar os titulares dos dados sobre vários assuntos, normalmente com antecedência e numa língua que é clara, concisa e acessível.

Há exceções ao direito – para exemplo, no contexto da investigação (sanitária e médica) ou de outras atividades de saúde pública.

Qualquer isenção ao direito a ser informado, no entanto, deve ser cuidadosamente avaliada e documentado.

Direitos dos Titulares de Dados

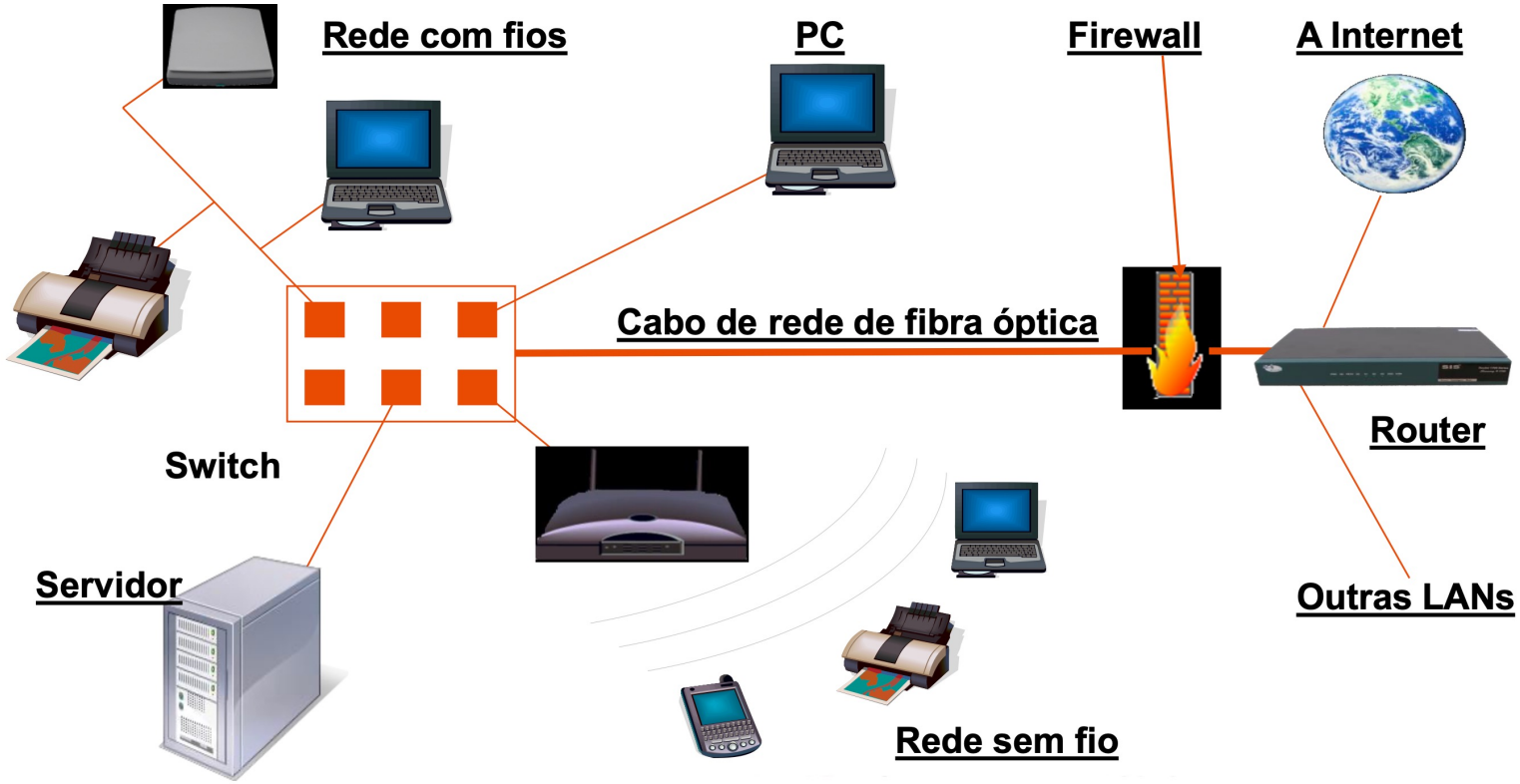
A instituição deve:

- Comunicar os direitos das pessoas em causa de forma clara e eficaz.
- Estabelecer processos e pontos de entrada para os pedidos das pessoas em causa.
- Assegurar parcerias com os titulares dos dados, que são os "clientes".
- Documentar os pedidos dos titulares dos dados e os esforços para os servir.
- Assegurar que os sistemas informáticos facilitam a adesão aos pedidos dos titulares dos dados (tais como a eliminação de dados).
- Desenvolver uma estratégia de comunicação sobre quaisquer razões para recusar pedidos de pessoas em causa.

Ameaças de Segurança

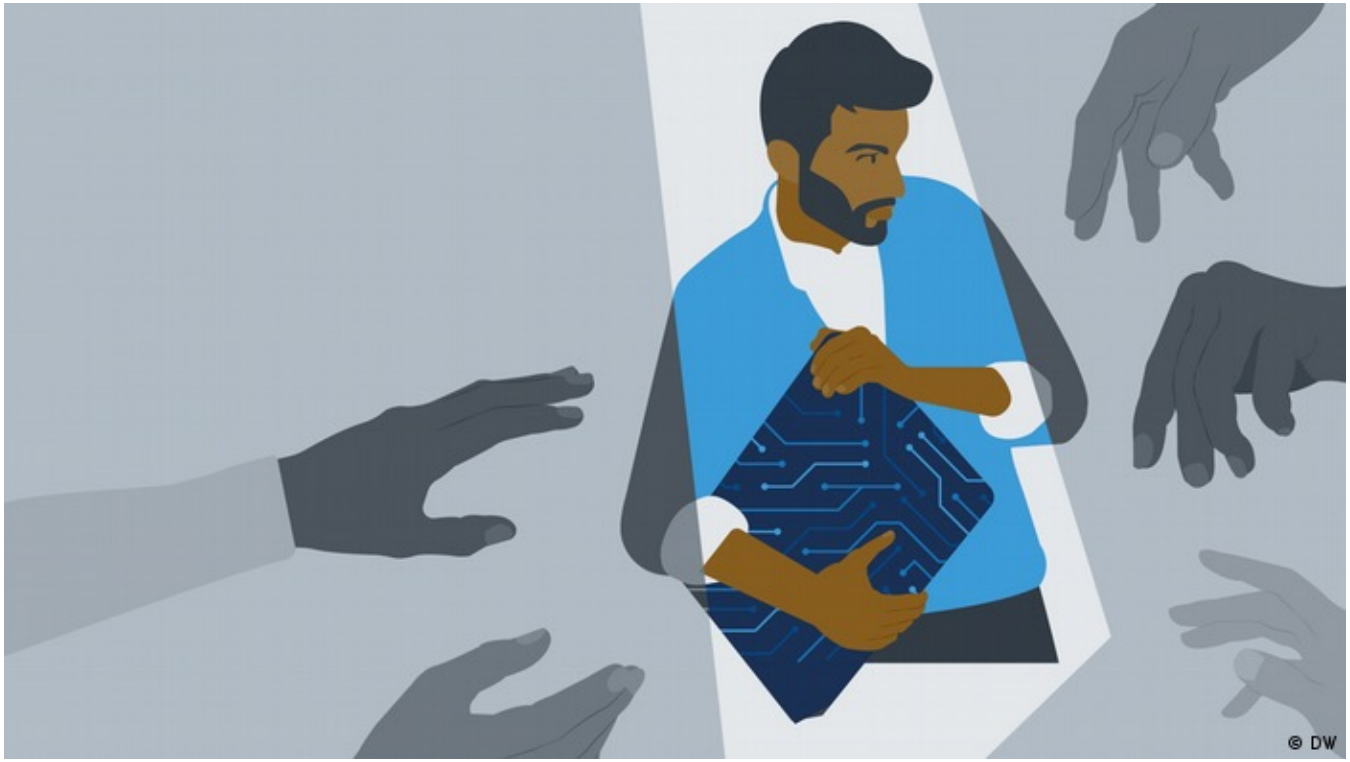
adaptado de: openEHR

Principais ameaças de Segurança e Privacidade



Exercício

Identificar **3** ameaças de Segurança e Privacidade dentro das instituições de saúde?



Principais ameaças de Segurança e Privacidade

Erro humano na identificação do paciente

- Associação incorrecta de dados de saúde de um paciente com outro.
- A incorreta identificação dos pacientes pode levar a que dados pessoais de um paciente entrem no registo de outro paciente.
- Violações da privacidade e possivelmente a erros clínicos.
- Um novo registo em vez do existente para o mesmo paciente, levando a dois ou mais registos clinicamente incompletes.

Como evitar?

Principais ameaças de Segurança e Privacidade

Erro humano na identificação do paciente

<u>Como evitar?</u>

- Identificação de 2 fatores (Nome complete e data de Nascimento).
- Utilização de identificador único do paciente (SNS/NIF/outro).
- Utilização de pulseiras de identificação com Código de Barras ou QR code.

Qual o identificador único de um utente dentro de uma unidade de saúde?

Principais ameaças de Segurança e Privacidade

Acesso inadequado por profissionais de saúde ou outros

- Acessos indevidos no ambiente de prestação de cuidados físicos.
- Acesso por qualquer trabalhador do hospital, não envolvido nos cuidados actuais do paciente.

Como evitar?

Principais ameaças de Segurança e Privacidade

Acesso inadequado por profissionais de saúde ou outros

Como evitar?

- Acões de sensibilização e responsabilização para eliminar a partilha de passwords.
- Incluir autenticação forte em todos os acessos a executar.
- Incluir sistemas de autologoff para evitar acessos indevidos.
- Adequar os SIS para garantir políticas de acesso por grupo profissional, âmbito, período e propósito.

- OpenEHR Dim

Principais ameaças de Segurança e Privacidade

Acesso inadequado por outras pessoas conhecidas do paciente

- Acesso indevido por um membro da família
- Acesso indevido por amigo ou conhecido

Como evitar?

Principais ameaças de Segurança e Privacidade

Acesso inadequado por outras pessoas conhecidas do paciente

<u>Como evitar?</u>

- Sensibilizar utentes para a problemática.
- Garantir a transparência e conhecimento ao utente no momento de acesso indevido à informação.

Principais ameaças de Segurança e Privacidade

Acesso indevido a dados de saúde por parte de empresas ou organizações.

Por exemplo, discriminação em atribuição de seguros de saúde.

Roubo malicioso ou acesso a dados de saúde (p. ex. de uma celebridade ou político) para fins lucrativos ou outros motivos pessoais

Ameaças genéricas à integridade e disponibilidade de dados, tais como vírus, worms, ataques de negação de serviço, etc

Falhas no software: devido a bugs, configuração incorrecta, falhas de interoperabilidade, etc.. Causa corrupção nos dados, ou visualização ou computação incorrecta, resultando em erros clínicos.

Principais ameaças de Segurança e Privacidade

Como evitar?

Implementação de politica de acessos;

Implementar barreiras de segurança que limitem security breaches.

Garantir desenvolvimento de SIS responsavel e orientado para a segurança e privacidade.

Ameaças de Segurança - Outros

- Não estar consciente de como armazenar dados corretamente.

- Cometer um erro no armazenamento da informação poderia ter sido evitado se se soubesse melhor o que é esperado por lei.

- Perder documentos contendo dados sensíveis sobre pessoas, quer estes estejam no seu computador.

- Divulgação inapropriada de dados pessoais.

- Correio eletrónico mal direcionado, resultando na perda ou exposição de informação sensível.

- Armazenamento não autorizado e acesso aos registos dos doentes.

Políticas de Proteção de Dados

adaptado de: WHO

Políticas de Proteção de Dados

A instituição deve:

- Definir e documentar medidas técnicas e operacionais.

- Definir e monitorizar os requisitos de segurança informática, idealmente com base nas melhores práticas como a Organização Internacional de Normalização (ISO) série 270XX.

- Estabelecer e manter uma gestão de identidade e acesso, assegurando os direitos de administrador e que deve seguir um conceito de "necessidade de saber".

- Assegurar que os dados sejam sempre encriptados, tanto em trânsito como em repouso.

Políticas de Proteção de Dados

A instituição deve:

- Avaliar e controlar regularmente a segurança informática - por exemplo, conduzindo terceiros testes de penetração.

- Desenvolver um procedimento em caso de violação de dados e uma estratégia de comunicação.

- Desenvolver um plano de recuperação de desastres, conforme necessário.

- Se aplicável, desenvolver uma estratégia de segurança para a utilização da computação em nuvem, em particular a utilização de nuvens públicas.

Disponibilidade

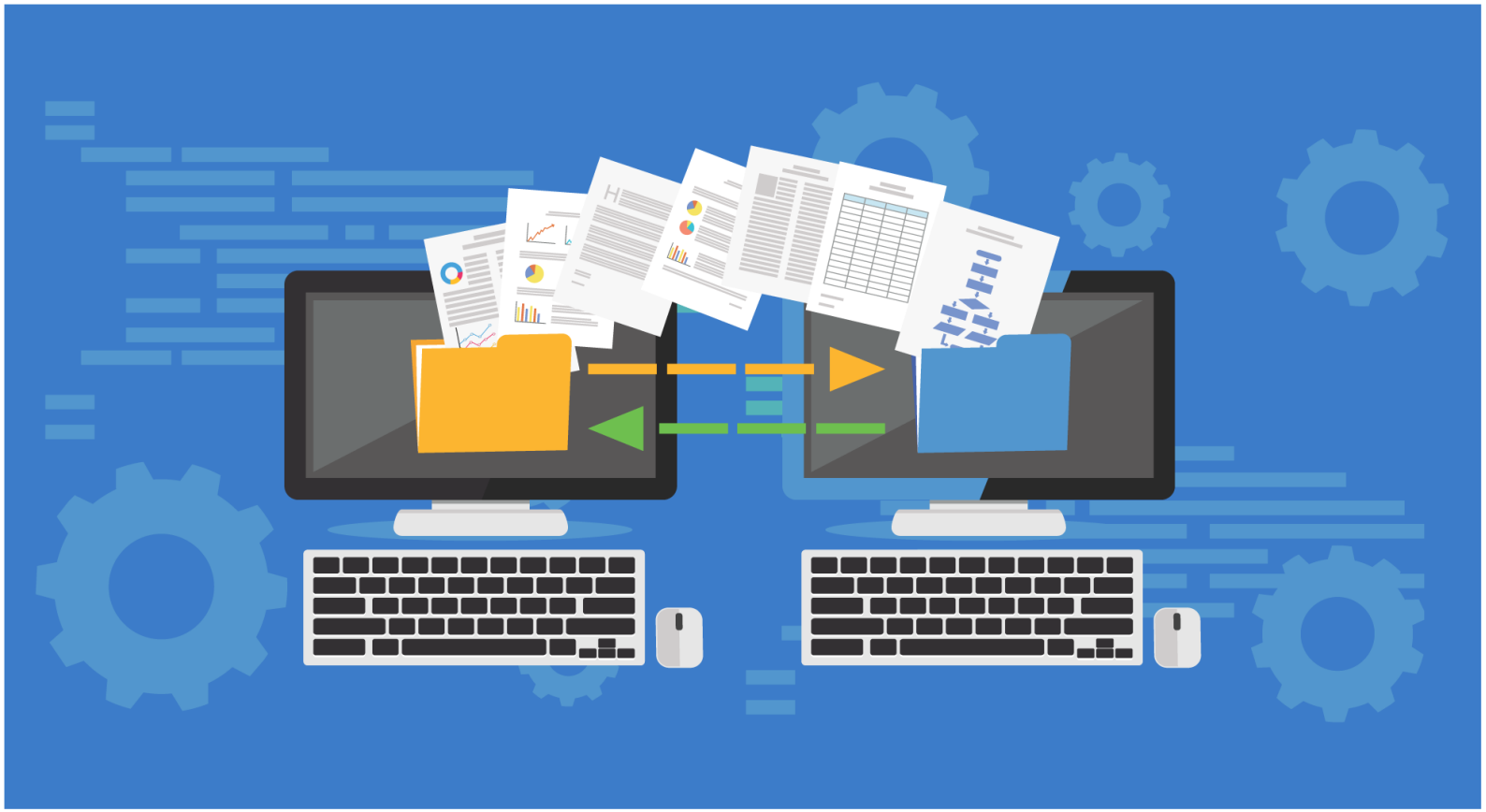
Disponibilidade

Definição:

- A informação está acessível ao pessoal autorizado sempre que for relevante.

- Trata-se de dar acesso à informação quando ela é necessária e, muitas vezes, num determinado context

Backups



Backups

- Garantir a salvaguarda em backup da informação da atividade do Hospital considerada relevante e existente nas aplicações, dos dados de configuração dos sistemas e do Software instalado.
- Identificar os ativos onde a informação classificada a salvaguardar reside;
- Definir a periodicidade com que devem ser efetuados backups;
- Definir os períodos de retenção dos backups;
- Definir a periodicidade da execução de testes de integridade de backups;
- Definir a periodicidade da execução de testes de reposição de backups;
- Definir o formato dos relatórios mensais resultantes da execução de backups e respetivos testes de integridade, execução, reposição e disponibilidade.

Disaster Recovery

Disaster Recovery

- Estabelecer um grupo de planeamento.
- Realizar uma avaliação de risco e definir **Objetivos de Ponto de Recuperação** (RPOs) e **Objetivos de Tempo de Recuperação** (RTOs) aceitáveis.
- Preparar um inventário dos ativos de TI.
- Identificar dependências e estabelecer prioridades.
- Desenvolver estratégias de recuperação.
- Elaborar um plano de comunicação.
- Elaborar documentação, critérios de verificação, procedimentos e responsabilidades.
- **Testar, testar, testar o plano!!**
- Implementar o plano.
- Manter a infraestrutura informática.

Processo de Gestão da Segurança de Informação

Processo de Gestão da Segurança de Informação

- **Prevenção:** Assegurar que os incidentes de segurança não acontecem. Definir normas simples e eficazes.

- **Deteção:** Deteção rápida e eficaz de incidentes que não podem ser previstos.

- **Correção:** Resposta de recuperação eficaz aos incidentes após a sua deteção.

Políticas de Segurança

- Devem ser corretamente definidas:
  - Normas gerais de acesso aos SI:
    - Atividades permitidas e atividades não permitidas
  - Normas para a atribuição de acessos
  - Normas para alteração de acessos
  - Normas para revogação de acessos
  - Normas para acesso à rede

Sistemas de Informação na Saúde