UNIVERSIDADE FEDERAL DO MARANHÃO - UFMA
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA - CCET
COORDENADORIA DO CURSO DE CIÊNCIA DA COMPUTAÇÃO – COCOM

MONIA TAINÁ TAVARES DE ARAUJO MENDES

SEGURANÇA DA INFORMAÇÃO DE DADOS MÉDICOS:
PROPOSTA DE MODELO HIERÁRQUICO DE CONTROLE DE RISCO
PARA PROTEÇÃO DE DADOS SENSÍVEIS

SÃO LUÍS
2023

MONIA TAINÁ TAVARES DE ARAÚJO MENDES

SEGURANÇA DA INFORMAÇÃO DE DADOS MÉDICOS:
PROPOSTA DE MODELO HIERÁRQUICO DE CONTROLE DE RISCO PARA PROTEÇÃO DE DADOS SENSÍVEIS

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Prof. Me. Carlos Eduardo Portela Serra de Castro

SÃO LUÍS

2023

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

Araújo Mendes, Monia Tainá Tavares de.
Segurança da informação de dados médicos : proposta de modelo hierárquico de controle de risco para proteção de dados sensíveis / Monia Tainá Tavares de Araújo Mendes. - 2023.
79 f.

Orientador(a): Carlos Eduardo Portela Serra de Castro.
Monografia (Graduação) - Curso de Ciência da Computação, Universidade Federal do Maranhão, São luís, 2023.

1. Controle de risco hierárquico. 2. Dados sensíveis. 3. Proteção de dados sensíveis. 4. Segurança da informação. I. Castro, Carlos Eduardo Portela Serra de. II. Título.

MONIA TAINÁ TAVARES DE ARAÚJO MENDES

SEGURANÇA DA INFORMAÇÃO DE DADOS MÉDICOS:
PROPOSTA DE MODELO HIERÁRQUICO DE CONTROLE DE RISCO PARA PROTEÇÃO DE DADOS SENSÍVEIS

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Prof. Me. Carlos Eduardo Portela Serra de Castro

Monografia aprovada em: ____/____/_____

_____

Prof. Me. Carlos Eduardo Portela Serra
Orientador

_____

Prof. Dr. Anselmo Cardoso de Paiva
1° Examinador

_____

Prof. Dr. Mário Antônio Meireles Teixeira
2° Examinador

A Luzivan Morais, pela paciência e incentivo ao gentilmente me guiar nos momentos finais deste trabalho.

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus, Senhor maior de toda minha fé. A meu namorado, Salviano Lima, por acreditar sempre nos meus sonhos, pelos momentos de paciência, gentileza e doação, por me acompanhar nessa caminhada e por todo o incentivo. Aos professores que puderam repassar com tamanho empenho todo o conhecimento necessário para que eu pudesse seguir firme nos meus ideais. Aos meus amigos, em especial Daniel, Felícia, César, Guilherme, Gabriel, Asan, Arthur e Luciano, pelos bons momentos de descontração e diversão, pela bondade em ajudar na minha trajetória sem desistir e pelo incentivo em momentos mais complexos do curso.

“Ninguém é suficientemente perfeito, que não possa aprender com o outro e, ninguém é totalmente destituído de valores que não possa ensinar algo ao seu irmão”

(São Francisco de Assis)

RESUMO

A utilização de dados sensíveis faz parte dos cenários médicos, sendo necessária para auxiliar profissionais da saúde na busca de melhores diagnósticos aos pacientes. Todavia, o tratamento dos dados sensíveis necessita de cuidados, visto que os mesmos englobam características restritas, que podem causar problemas aos usuários em casos de exposição. A ideia de gerenciar riscos de dados sensíveis através da utilização de uma estrutura hierárquica ajuda na tomada de melhores decisões, partindo em níveis que melhor assegurem os dados sensíveis. Esse trabalho tem o intuito de ilustrar um modelo hierárquico de controle de risco, para ser utilizado em cenários que lidam exclusivamente com dados sensíveis, auxiliando na tomada de medidas que melhor protejam esses dados.

Palavras-chave: Dados sensíveis. Controle de risco hierárquico. Segurança da informação. Proteção de dados sensíveis.

ABSTRACT

The sensitive data utilization is part of medical scenarios and is necessary to assist health professionals in the search for better patients diagnosis. However, the sensitive data treatment needs care, since they include restricted characteristics, which can cause problems for users in exposure cases. The idea of managing sensitive data risks through the use of a hierarchical structure helps in decision making better decisions, starting at levels that better secure sensitive data. This job is intended to illustrate a hierarchical model of risk control, to be used in scenarios that deal exclusively with sensitive data, helping to take measures that better protect that data.

Keywords: Sensitive data. Hierarchical Risk Control. Information Security. Sensitive Data Protection.

LISTA DE ILUSTRAÇÕES

Figura 1 - Exemplo de ciclo de vida dos dados no setor da saúde 20
Figura 2 - Objetivos da análise de risco 23
Figura 3 - Exemplificação estatística de vazamentos de dados no mundo.....25
Figura 4 - Modelo de controle de risco HOC 26
Figura 5 - Tríade CIA 38
Figura 6 - Diagrama de ameaças 41
Figura 7 - Exemplo de Phishing por e-mail.....42
Figura 8 - Ransomware Petya.....44
Figura 9 - Organograma - Empresa Med&Clinic.....49
Figura 10 - Ciclo de dados - clínica Med&Clinic 50
Figura 11 - Hierarquia de controle de risco - Fluxo de entrada e coleta dos dados 59
Figura 12 - Hierarquia de controle de risco - Fluxo de conscientização
e treinamento colaborativo 60
Figura 13 - Hierarquia de risco - fluxo de armazenamento.....61
Figura 14 - Hierarquia de risco - fluxo de compartilhamento.....63
Figura 15 - Hierarquia de risco - fluxo de acessos 64
Figura 16 - Possíveis controles e aplicabilidades do controle de risco hierárquico 65

LISTA DE TABELAS

Tabela 1 - Processos de transformação de dados a informação.....18
Tabela 2 - Exemplos de direcionamento de dados pessoais coletados.....19
Tabela 3 - Comparativos de um controle de risco organizado e não organizado.....28
Tabela 4 - Características dos documentos físicos e digitais.....34
Tabela 5 - Tabela das três idades do ciclo documental 35
Tabela 6 - Ações e riscos no ambiente sensível 40
Tabela 7 - Análise de ativos - Clínica Med&Clinic 53
Tabela 8 - Classificação de ativos - Clínica Med&Clinic 54
Tabela 9 - Classificação de vulnerabilidades: Clínica Med&Clinic.....55
Tabela 10 - Avaliação dos riscos - Clínica Med&Clinic.....56

LISTA DE ABREVIATURAS E SIGLAS

ENAP	Escola Nacional de Administração Pública
GDPR	General Data Protection Regulation
HOC	Hierarchy of Controls
HTTPS	Hyper Text Transfer Protocol Secure
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
OECD	Organization for Economic Cooperation and Development
PII	Personally Identifiable Information
SGSI	Sistema de Gerenciamento de Segurança da Informação
SGSSO	Sistema de Gestão de Saúde e Segurança Ocupacional
WIFI	Wireless Field

SUMÁRIO

1 INTRODUÇÃO 14
1.1 Motivação/ justificativa 14
1.2 Objetivo Geral 16
1.2.2 Objetivos específicos 16
1.3 Metodologia 16
2 DADO E INFORMAÇÃO 17
2.1 Conceitos e termos 17
2.2 Coleta de dados e operações 18
2.3 Dados pessoais e dados sensíveis 20
2.4 Problemas relacionados ao armazenamento e manipulação de dados sensíveis 21
2.5 Análise de risco e métodos paliativos para proteção de dados 22
2.5.1 Processos paliativos na proteção de dados 23
2.6 Controle de risco 25
2.6.1 Escolha de organização hierárquica para proteção de dados sensíveis e benefícios 27
3 GESTÃO E PROTEÇÃO DE DADOS SENSÍVEIS 29
3.1 História da proteção de dados 29
3.1.1 Regulamentação geral da proteção de dados - RGPD 29
3.2 Histórico de proteção dos dados no Brasil e a lei geral de proteção de dados - LGPD 31
3.3 Gestão documental e operações de dados 33
3.4 Relação das Normas ISO 27001, 27701 e 27002 com a proteção de dados sensíveis 35
3.4.1 ISO 27001 36
4 RISCOS DE SEGURANÇA RELACIONADOS AOS DADOS SENSÍVEIS 38
4.1 Tríade CIA 38
4.2 Risco, vulnerabilidade e ameaças 39
4.3 Ameaças intencionais e não intencionais aos dados sensíveis 41
4.3.1 Phishing 42
4.3.2 Ransomware 43
4.3.3 Risco humano e engenharia social 45
4.3.4 Ameaças naturais e ameaças não intencionais 45

4.4 Proteção de documentos e gestão documental **46**
5 ESTUDO DE CASO **49**
5.1 Apresentação da empresa fictícia e cenário principal **49**
5.1.1 Fluxos e ciclo de vida dos dados sensíveis - Clínica Med&Clinic *50*
5.1.2 Vulnerabilidades no fluxo de dados - Clínica Med&Clinic *51*
5.2 Análise e avaliação de risco - Clínica Med&Clinic **52**
5.2.1 Identificação e classificação dos ativos *53*
5.2.2 Identificação das vulnerabilidades *54*
5.2.3 Avaliação dos riscos nos processos *55*
5.2.4 Controle ou aceitação do risco *56*
6 MODELO PROPOSTO **59**
6.1 Modelo proposto de controle de risco hierárquico - Clínica Med&Clinic **59**
6.1.1 Fluxo de entrada e coleta dos dados sensíveis *59*
6.1.2 Fluxo de conscientização e treinamento colaborativo *60*
6.1.3 Fluxo de armazenamento dos dados sensíveis *61*
6.1.4 Fluxo de compartilhamento dos dados sensíveis *62*
6.1.5 Fluxo de acessibilidade aos dados sensíveis *64*
6.2 Aplicabilidade do modelo hierárquico de controle de risco - Clínica Med&Clinic **65**
7 CONCLUSÃO **66**
REFERÊNCIAS **68**
APÊNDICE **74**
ANEXOS **78**

1 INTRODUÇÃO

Com a inserção cada vez mais de dispositivos e sistemas computacionais, dados começaram a ser suportados e ofertados em sistemas de informática, assegurando vantagens em relação ao modelo não computadorizado. Fatores benéficos como a integração entre a comunicação, agilidade em processos e o gerenciamento tornaram o modelo sistemático tecnológico muito mais vantajoso para se utilizar, tanto em pequenos ou médios grupos organizacionais.

Em ambientes hospitalares e clínicas, a utilização de sistemas que permitissem gerenciar informações de pacientes também contribuíram para agilizar processos e ações. Dados podem ser integrados, armazenados e utilizados, deixando as atividades mais favoráveis e trazendo benefício na qualidade prestada aos pacientes. Entretanto, todo esse conjunto de dados médicos possui em comum diversas informações bastantes extensas de determinado indivíduo, informações estas extremamente sigilosas. Os dados médicos informam, por exemplo, sobre o estado de um paciente ou condição atual e é perceptível que as violações desses dados podem trazer consequências muito sérias.

Dados médicos são caracterizados como dados sensíveis, conforme a LGPD (lei geral de proteção de dados - artigo 5, inciso 2, parágrafo único), e, portanto, exigem proteção mais restrita do que os dados pessoais. Com a utilização de mecanismos tecnológicos cada vez mais alinhados às operações médicas, surgem dúvidas em relação à manipulação, armazenamento e proteção desses dados.

O gerenciamento de risco provê diversas formas de proteger diversos dados, inclusive os sensíveis. Como existem diversos procedimentos com o objetivo de mitigar perdas referentes aos dados, é interessante definir práticas e estratégias estruturalmente organizadas para trazer maior segurança ao cenário de dados sensíveis.

1.1 Motivação/ justificativa

A ideia do controle de risco impõe medidas que podem ser sugeridas com o objetivo de se precaver em determinadas situações de perda de dados. Mesmo que os sistemas de proteção e seus métodos não sejam 100% seguros, a identificação de falhas relacionadas ao manuseio e armazenamento de informações torna-se uma etapa muito importante para se traçar qualquer procedimento futuro de proteção de dados.

O registro clínico se resume a campos de informações relacionados de um paciente, sendo realizados tanto de forma manuscrita como computadorizada. As funções do registro são muitas, como auxiliar o tratamento dos pacientes, servir de base administrativa ao facilitar os processos internos dos setores ou favorecimento da pesquisa e organização de documentos legais de atuação médica (LOBO, 2006).

Abrangendo o conjunto de dados pessoais, o subconjunto de dados sensíveis possui como característica informações adicionais, como dados étnicos, biométricos ou religiosos. Dados sensíveis exigem maior cautela tanto na manipulação quanto no armazenamento, uma vez que o vazamento desses dados pode trazer consequências diretas aos direitos de proteção fundamentais do cidadão, ocasionando discriminação, por exemplo.

Conforme Morsch (2020) na área médica é obrigatório o armazenamento de procedimentos médicos em prontuários como exames, *anamnese* (entrevista a qual o profissional de saúde realiza com o objetivo de avaliar o ponto inicial do diagnóstico de uma doença) ou resultado de exames, e, portanto, é necessário que a clínica defina a finalidade desses dados, o manuseio e armazenamento, além do compartilhamento com outras clínicas em si.

A prevenção de risco deve ocorrer considerando qualquer vulnerabilidade que esteja aparente em um sistema ou setor. Desta análise também é possível prever cenários onde possam ocorrer situações desvantajosas aos dados armazenados. Nessa relação de manuseio de cenário e vulnerabilidade pode-se definir iniciativas que sejam mais precisas para trazer segurança de dados, minimizando vazamentos, ou perdas, por exemplo.

Práticas atuais como atualizações de sistemas recentes, treinamento de colaboradores, proteções relacionadas a *phishing* e *e-mails* danosos ou verificações em duas etapas são metodologias válidas para se iniciar a proteção de dados sensíveis. Inúmeros fatores podem ser considerados, entretanto a falta de organização nas tomadas de gestão pode deixar que critérios importantes passem sem serem percebidos. Entende-se que considerar uma hierarquia de controle de risco é uma boa maneira intuitiva de visualização, partindo do modelo em uma "base" e subindo a determinado nível para se garantir um passo inicial de segurança. Isso contribui para tornar a tomada de decisão mais estruturada e organizada.

Neste cenário de vulnerabilidade, este trabalho visa ilustrar tomadas de procedimentos utilizando um modelo hierárquico de risco, ao qual foi escolhido por ser estruturalmente intuitivo e de fácil visualização, permitindo que sejam tomadas decisões específicas gradativas aos quais tem o objetivo de proteção, operação e manuseio de dados sensíveis.

1.2 Objetivo Geral

Propor um modelo hierárquico de adoção de medidas de controle de risco para proteção de dados sensíveis.

1.2.2 Objetivos específicos

- Descrever vulnerabilidades de risco relacionadas ao manuseio, armazenamento e operação de dados.
- Selecionar técnicas de proteção que melhor se comportem com dados sensíveis.
- Estruturar hierarquicamente as práticas de controle selecionadas.

1.3 Metodologia

Este trabalho baseia-se em uma estratégia descritiva e qualitativa, onde os conceitos dos capítulos iniciais se darão por pesquisa bibliográfica. Estes dados serão baseados conforme informações analisadas pela LGPD (Lei geral de proteção de dados), ISO 27001 (sistema de gestão da segurança da informação), ISO 27005 (gestão de riscos de segurança da informação), referências da *internet* e os fundamentos de segurança da informação (HINTZBERGEN et al. 2018).

A metodologia inicial abrangerá contextos referentes a dados, tipos de ataques, riscos e seus impactos referentes às informações classificadas como dados sensíveis. A partir dos conceitos iniciais, serão estruturados os “passos” que serão abordados como sugestão para proteção destes dados. A abordagem dos critérios iniciais será fundamental para construção do modelo de procedimento hierárquico.

Decidiu-se aplicar parte do estudo de caso da construção das etapas de gestão de risco em uma clínica médica fictícia. Esta empresa será criada e detalhada em relação ao processo de tratamento de dados, políticas internas e práticas de segurança, para ter aplicados os métodos de gestão hierárquicos presentes neste trabalho. A preferência pelo cenário de uma clínica médica se deve principalmente pelas atividades que envolvem operações de dados de caráter sensível.

2 DADO E INFORMAÇÃO

2.1 Conceitos e termos

Usualmente percebemos que informações e dados participam de uma infinidade de situações, sendo utilizados para descrever determinados elementos ou orientar tomadas de decisões. Na necessidade de se obter conhecimento e compartilhá-lo, a manipulação, armazenamento e disseminação dos dados e informações tornou-se comum.

Ao participarem juntamente no contexto informativo, dados e informações são definidos por diversos conceitos, sendo tratados erroneamente como sinônimos. Conforme Silva e Gomes (2015) a informação tem conquistado espaços entre indivíduos, grupos, empresas e sociedade de forma ampla, porém a complexidade e variedade de conceitos tem promovido uma diversidade de significados a dados e informações, dificultando a construção de sentidos mais consistentes.

Elias (2017) diferencia que dados são caracterizados por não possuir significado relevante inicialmente, ou seja, por si só não tem valor para fundamentar conclusões isoladas. Porém a partir da ordenação e organização dos dados passamos a obter o valor informacional, sendo que a consolidação dos dados gera a fundamentação do conhecimento e compreensão dentro de um determinado contexto.

> Os dados não falam por si. Eles são como uma matéria prima, sobre a qual trabalhamos (juntando-os, correlacionando-os, contrapondo-os etc.) buscando produzir informações que se traduzam em um conhecimento, uma interpretação e um juízo sobre uma determinada situação. A partir da combinação de dados gera-se informações e elabora-se uma interpretação. Pode-se entender esta interpretação como uma avaliação (ou seja, valia = dar valor), buscando-se construir um conhecimento e a formar um juízo sobre determinada situação. Necessariamente, este juízo incorpora as concepções, os pressupostos, os valores e as referências que fundamentam a visão de mundo do sujeito que interpreta a situação. (FERREIRA, 1999, p. 3)

De forma ampla, dados são a representação significativa de um valor primitivo quantitativo ou qualitativo, responsável por ser a “base” da informação. Não possuindo significado relevante inicialmente, os dados se abstém do valor responsável por fundamentar conclusões. A informação, por sua vez, é a organização dos dados, possuindo como objetivo a transmissão de determinado conceito. Para que o dado passe a ser informação, Nascimento, Tóffolo e Tomaél (2011) explicam que ele precisa ser significativo, sendo assimilado conforme disponibilidade e interesse do usuário e a partir da assimilação, passe a ser convertido em informação.

Tabela 1 - Processos de transformação de dados a informação

Processo da informação	Dado	Informação
Vinculação	000.000.000.00	O dado é um CPF? Um valor financeiro?
Decodificação	TGAO	A palavra seria gato?
Abstração	Manga	Fruta ou parte da roupa?

Fonte: A autora (2022)

2.2 Coleta de dados e operações

A coleta de dados faz parte do cenário habitual, onde geralmente são importantes os conjuntos coletados para dispor informações. Inúmeras organizações necessitam coletar dados para poder desempenhar serviços, criar recomendações para usuários, ou armazenar informações que serão importantes para processos futuros. No *marketing*, dados são essenciais, visto que coletar informações de um público alvo pode, por exemplo, economizar recursos da organização ao concentrar investimentos para fins específicos, tudo isso através da transformação do processo em indicadores[1]. Dados indicam quem compra o produto, quem o acessa e para qual grupo específico será direcionado.

Em setores comerciais, ao se fazer um cadastro de um cliente (por formulários de contato, assinaturas de *newsletter* ou cadastros simples), ocorre a "transmissão" de dados, onde são fornecidas diversas informações pessoais. Essas informações irão permitir, por exemplo, a oferta de determinado serviço particular baseado na localização, cupons promocionais baseado em características pessoais, etc.

Mesmo quando a coleta de dados seja grande parte das vezes vinculada a processos virtuais, coletas físicas também fazem parte do conjunto de operações realizadas com o intuito de se criar possibilidades para ações de relacionamento e *marketing*. Lorecchio (2020), destaca que embora no cenário atual comércios eletrônicos realizados por meio de plataformas *online* tenham grande presença, existem ainda o comércio em formato tradicional, onde realizam o ativo estratégico da "fidelização". Essa fidelização, que é realizada através da coleta de cadastros que normalmente necessitam de nome completo, data de nascimento, CPF e telefone,

[1] **A importância da coleta de dados para um marketing inteligente.** https://blog.allin.com.br/coleta -de-dados/

geram a vinculação da compra com um perfil, permitindo por exemplo, o recebimento de novidades na loja ou ofertas.

Tabela 2 - Exemplos de direcionamento de dados pessoais coletados

Tipos de dados	Aplicabilidade de dados
Sexo	Direcionamento de um produto (roupa, cosméticos, objetos domésticos)
Data de nascimento	Cupom de fidelização por aniversário
CPF	Análise de crédito, identificação de cliente
Localização	Direcionamento de promoções conforme loja mais próxima

Fonte: A autora (2022)

Analisando a área da saúde, a coleta de dados constitui-se de um mecanismo também essencial, com propósito qualitativo e quantitativo, e assim como no *marketing*, possui fator estratégico para os setores de saúde. O gerenciamento de dados na saúde concentra-se boa parte na identificação dos pacientes, o que facilita na busca de informações e auxilia na criação de prontuários e outros documentos. Além dos dados pessoais, a análise de dados médicos como históricos, hábitos ou enfermidades torna-se necessária na obtenção de diagnósticos, podendo evitar custos altos, sem comprometer a eficácia e qualidade do tratamento.[2]

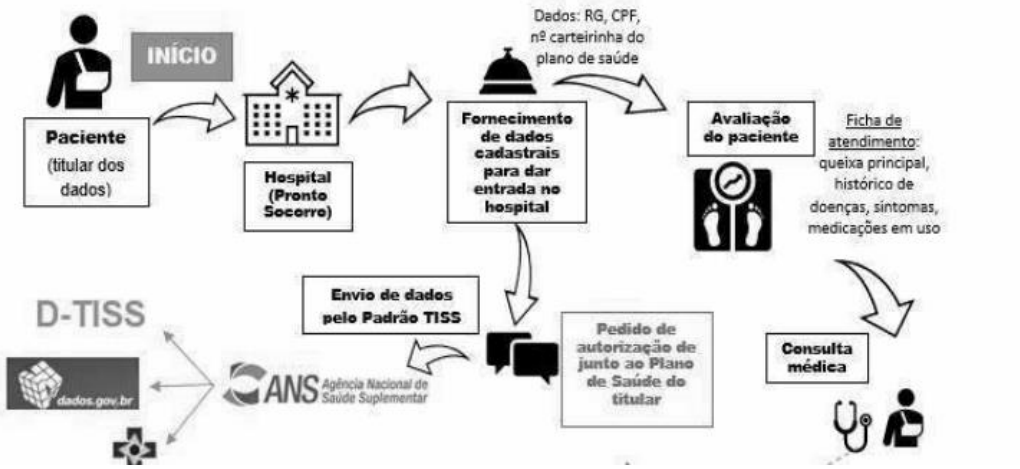
Para os profissionais de saúde, entender as informações tornam a relação clínica muito mais adequada, necessitando que estes profissionais passem a assumir o papel de "clínico investigador". Além dos dados pessoais, as experiências de vida e informações específicas de um paciente coletadas ajudarão a compreender profundamente problemas relacionados à saúde e vida, auxiliando a se chegar a um diagnóstico (CAMPOS; FONTANELLA; TURATO, 2006, p. 2).

Em hospitais e clínicas, além dos profissionais de saúde, outros profissionais coletam diversos dados dos pacientes, com o intuito de facilitar a rotina do estabelecimento médico. Operacionalmente, o processo de tratamento e coleta de dados inicia-se desde sistemas de agendamento ou gestão integrada, passando a compor diversas operações necessárias (resultado

[2] **Conheça agora a importância da análise de dados em saúde**. Https://toccato.com.br/blog/conheca-agora -a-importancia -da-analise-de-dados-em-saude/.

de exames, *anamnese*, diagnóstico, evolução do paciente, etc.) O que se observa é que na trajetória dos dados nos serviços de saúde, desde o momento inicial (recepção), até as atividades médicas e seus resultados, foram coletados, armazenados e operados diversos tipos de dados, todos eles envolvendo informações importantes, associadas diretamente a um paciente.

Figura 1 - Exemplo de ciclo de vida dos dados no setor da saúde



Fonte: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao- Dados-Prestadores-Privados-CNSaude_ED_2021.pdf (2021).

2.3 Dados pessoais e dados sensíveis

A partir do momento em que dados poderiam ser vinculados à identificação de um determinado indivíduo, passaram a ser caracterizados como informações de identificação pessoal (PII - *Personally Identifiable Information* ou simplesmente dados pessoais). *Os* PII são as representações informatizadas que permitem direcionar a identificação direta ou indireta de uma pessoa natural, como nome completo, CPF, endereços ou *e-mails.* [3]

São considerados dados de critério pessoal:

- Dados que relacionam o indivíduo, como nome completo, cadastro de pessoa física (CPF) e registro de nascimento (RG).
- Endereço (assim como outros dados de localização como GPS e endereço IP).
- *E-mail* e número de telefone.
- Dados trabalhistas, como renda, histórico de pagamentos ou número de cartão bancário.

[3] U.S. DEPARTMENT OF LABOR. **Guidance on the Protection of Personal Identifiable Information**. https://www.dol.gov/general/ppii#:~:text=Personal%20Identifiable%20Information%20(PII)%20is,either%20direct%20or%20indirect%20means.&text=It%20is%20the%20responsibility%20of,to%20which%20they%20have%20access.

- Fotografia pessoal.

Dentro do conjunto dos dados pessoais existem aqueles que possuem uma característica acrescida relacionada a revelações “extras”, correspondendo a informações legislativas que podem estar relacionadas a vulnerabilidades de discriminação. Estes tipos de dados são denominados como sensíveis.

Dados sensíveis podem ser definidos como:

- Origem racial e étnica.
- Convicção religiosa, filiação a sindicatos, opinião política ou filosófica.
- Dado referente a vida sexual.

Na saúde, os dados considerados sensíveis são aqueles relacionados a doenças, deficiências, riscos de doenças, relatórios médicos, prontuários e resultados de exames, assim como dados biométricos e informações genéticas (CONFEDERAÇÃO NACIONAL DA SAÚDE, 2021, p. 46)

2.4 Problemas relacionados ao armazenamento e manipulação de dados sensíveis

Observando o exemplo do ciclo médico, é fácil notar que no armazenamento e operação, praticamente boa parte dos dados são considerados sensíveis. Nas clínicas médicas os pacientes são registrados em cadastros, muita das vezes gerenciados por sistemas digitais que permitem funcionalidades como agendamento ou a interligação com o paciente/médico (para geração de laudos ou diagnósticos). Além dos sistemas de gerenciamento médico, a criação de documentos físicos com informações sensíveis também faz parte do cenário da saúde, como no prontuário médico e fichas de *anamnese*.

Imaginando o ciclo médico constrói-se a seguinte representação: na recepção, o titular geralmente necessita informar dados pessoais para o cadastro inicial (nome, CPF, número de plano de saúde). Após a recepção, passando por um processo de “entrevista” (anamnese), o titular é questionado acerca de algumas informações sensíveis (como alergias, transtornos e históricos de doenças), sendo que esses dados serão registrados em um prontuário. Perceba que nesse documento podem ser incluídas informações sensíveis não somente dos titulares, mas também dos familiares para fins de análise externa.

Com o grande volume transitado de dados sensíveis, o questionamento relacionado ao cuidado desses tipos de dados torna-se indiscutível. Um risco relacionado à operação está

baseado no vazamento desses dados. Em mãos erradas, a exposição de dados sensíveis do titular torna-se prejudicial.

> Ademais, veja-se que entre o registro do paciente na recepção e a consulta médica foram coletados e armazenados diversos dados pessoais e sensíveis, além de outras informações que serão geradas e posteriormente tratadas quando da realização dos exames adicionais. Dessa situação quotidiana dos prestadores de serviço de saúde diversas outras questões são suscitadas: em quais momentos os dados do paciente (titular) foram tratados ao longo de todos os procedimentos aos quais ele foi submetido? O compartilhamento dos exames entre laboratório e hospital precisam do consentimento do paciente? Quais os direitos do paciente em relação aos seus dados e quais as obrigações do hospital e laboratório? (CONFEDERAÇÃO NACIONAL DA SAÚDE, 2021, p. 49)

Dados sensíveis, por sua vez, tratam de características mais íntimas de um usuário. Sendo assim, as principais consequências relacionadas à falta de proteção dos dados sensíveis estão relacionadas à exposição do titular dos dados, afetando tanto a vida pessoal quanto a vida profissional. Um exemplo é de um usuário que pode ser demitido ou não ser inserido em meio trabalhista ou social por determinada deficiência física, ou por alguma condição médica específica, como portadores do vírus HIV (aspectos de segurança de dados serão melhor abordados no cap. 3).

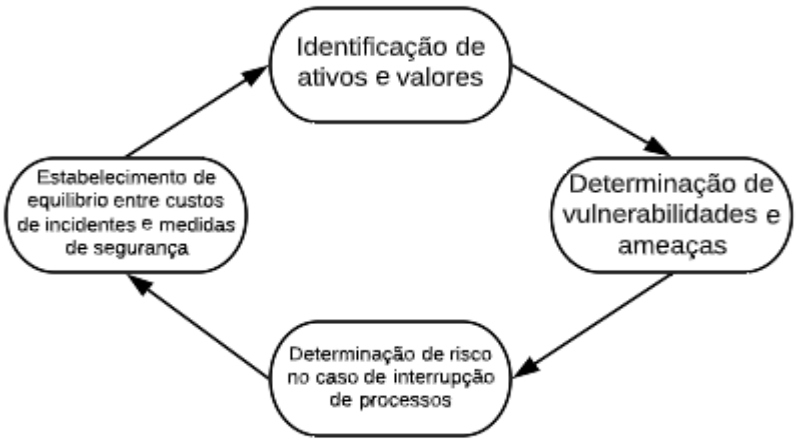
2.5 Análise de risco e métodos paliativos para proteção de dados

Inicialmente, para a aplicação e controle de operações que protejam dados em uma organização, é imprescindível definir um processo de análise de risco. Conforme a norma ISO 27005, o risco é definido como um efeito da incerteza nos objetivos, um “desvio” em relação a um resultado esperado. A análise de risco, portanto, é o processo de definição e compreensão do cenário do risco, onde será determinado o nível do mesmo (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011).

Ao se realizar uma análise de risco, aborda-se quais ameaças são mais importantes, identificando os riscos, para enfim tomar as medidas mais apropriadas. Hintzbergen et al. (2018), exemplifica que diversos objetivos são garantidos ao se realizar a análise de risco, como:

- Alinhar os objetivos de uma organização entre o TI e os objetivos da empresa.
- Esclarecer as ameaças relevantes.
- Garantir a implantação das medidas de proteção de uma forma mais eficiente e econômica.

Figura 2 - Objetivos da análise de risco [4]



Fonte: Hintzbergen et al (2018).

Entretanto é importante enfatizar que mesmo para especialistas em segurança, a tomada de decisão necessária para se encontrar o ponto de equilíbrio entre medidas de segurança muito restritivas ou eficazes não é fácil. A análise de risco vem para ajudar no estabelecimento de medidas de segurança efetivas e equilibradas, tanto envolvendo o equilíbrio da aplicação da medida, quanto o seu custo para a organização (HINTZBERGEN et al. 2018).

Ao se analisar melhor os riscos e definir grupos de abordagem (qualitativo ou quantitativo)[5], as contramedidas de segurança tornam-se mais efetivas de serem aplicadas.

> Exigências legais para a proteção de dados podem, por vezes, forçar as empresas a tomar medidas que realmente custem mais do que o valor dos ativos que estão sendo protegidos. Além disso, pode ser difícil determinar o valor dos dados[...]. Uma análise de risco puramente quantitativa é praticamente impossível. Uma análise quantitativa do risco tenta atribuir valores a todos os aspectos, mas isso nem sempre é possível[...]. Mas tente dar um valor ao dano causado a minha empresa. Quanto uma empresa perde quando certos dados são perdidos? Pode ser impossível determinar isso em algumas ocasiões, mas nem sempre. Isso pode tornar difícil determinar as medidas corretas para prevenir danos.
> (HINTZBERGEN et al. 2018, p. 34)

2.5.1 Processos paliativos na proteção de dados

[4] Análise de risco conforme objetivos descritos por Hintzbergen et al (2018, p.34), com criação de fluxograma pela autora.

[5] Uma análise quantitativa de risco tem como objetivo calcular, com base no impacto do risco, o nível do prejuízo financeiro e a probabilidade de uma ameaça se tornar um incidente. Uma análise de riscos puramente quantitativa é praticamente impossível. Uma análise quantitativa do risco tenta atribuir valores a todos os aspectos, mas isso nem sempre é possível.
Na análise qualitativa, em vez de números e valores, os métodos caminham através de diferentes cenários de possibilidade de risco e classificam a gravidade das ameaças e a validade das possíveis contramedidas (HINTZBERGEN et al. 2018, p. 35).

Conforme visto, a análise de risco deve ser definida antes para que se conheça o cenário de vulnerabilidades, e a partir disso sejam traçadas medidas para a resolução dos problemas. Pular a análise e escolher uma ordem de soluções não organizada para assegurar os dados pode tornar o processo de resolução mais custoso, ineficiente ou apenas mitigante.

Até então, a ordem no processo de proteção de dados é adotada pelas organizações de forma independente, possuindo uma análise centralizada, sem ordem específica de resolução do risco. Embora o contexto de proteção de dados esteja diretamente ligado com o dia a dia das organizações, algumas recorrem à proteção de forma mais "frágil" utilizando métodos temporais (para mitigar um problema recente), ou cedendo grande acesso por confiança, sem a designada função. Esses processos, definidos como processos paliativos, são atividades desenvolvidas com o intuito de se proteger dados, porém sem ocasionar grande demanda organizacional. Observa-se, portanto, que alguns fatores são levados em consideração na escolha de métodos paliativos, muita das vezes sendo escolhidas as opções mais fáceis, acessíveis e de baixo custo:

- **Escolha de sistemas de gestão de qualidade média/baixa em relação a segurança:** Softwares de gestão são analisados conforme complexidade e disponibilidade de funções, porém boa parte das vezes não são analisados em relação à proteção dos dados. O preço demandado também é um motivo da falta de aquisição em organizações pequenas e médias.
- **Proteção apenas dos dispositivos “fixos”:** Algumas organizações utilizam a proteção de dados para dispositivos fixos (*desktop*), esquecendo dos dispositivos móveis.
- **Treinamento escasso; Redirecionamento não abordado a toda a organização:** Também ocasionado pelo custo e falta de instrução da organização. O redirecionamento incompleto (apenas em alguns setores) gera uma oportunidade fácil para ataques contra os dados, já que cuidados básicos sobre políticas de segurança passam despercebidos.
- **Gestão de acesso facilitada:** Um fator que não é considerado em algumas organizações é o fator de papel da gestão. Muitas das vezes são facilitados os processos de acesso a colaboradores devido a fatores de convivência e afinidade ou porque não há a designação correta de funcionários/demanda. A abordagem humana em relação aos dados, tanto físicos quanto digitais, também é um fator que deve ser analisado na gestão de controle e segurança dos dados (fatores relacionados à colaboração humana em operação a segurança serão melhor abordados no cap. 4).

Além desses quesitos, não ter um mapeamento constante de vulnerabilidades e atuar apenas quando acontecem ameaças é um grande problema, visto que esse tipo de resposta limita as opções de proteção aos dados. Novas modalidades de trabalho (como o *home office*) aumentaram a preocupação com a segurança, visto que metade dos lares brasileiros não possuem proteção ao acesso *wifi*[6], podendo ocasionar a invasão da rede e coleta de informações da organização. Ataques agressivos (como os de *ransomware*) também geram preocupação, e por isso é importante reforçar que cobrir todas as possíveis vulnerabilidades (tanto humanas quanto de dispositivos) e investigar todas as falhas para impedir danos futuros são as formas mais corretas de atuação (SAVELLI, 2021).

Figura 3 - Exemplificação estatística de vazamentos de dados no mundo

Fonte: https://www.lb2.com.br/blog/vazamento-de-dados (2021)

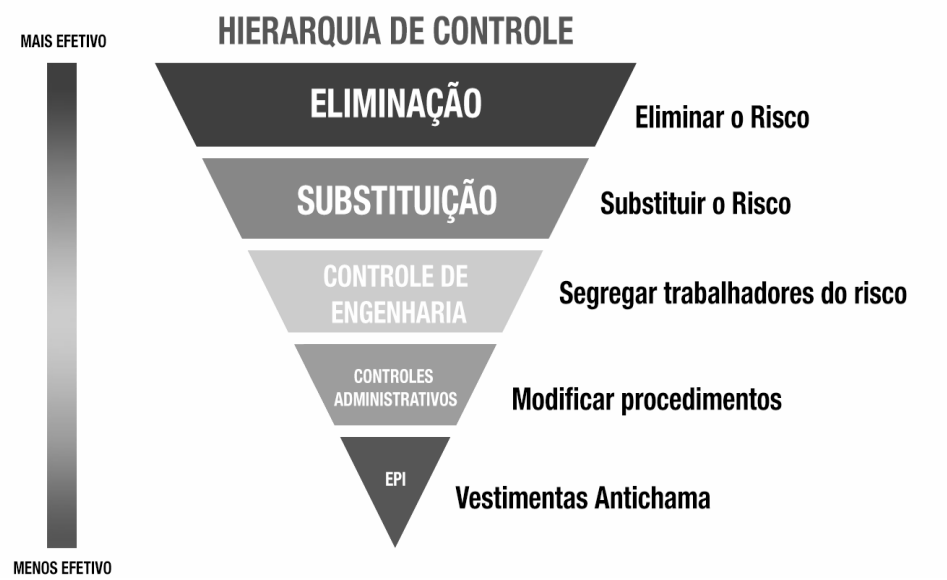
2.6 Controle de risco

Controles ou tratamentos de risco são processos especiais que têm o objetivo de atuar sobre os riscos já existentes, trazendo equilíbrio na organização. Fernandes (2009) explica que o tratamento de risco é a fase da gestão onde envolve a escolha de controles que serão utilizados para as operações de evitar, mitigar ou aceitar os riscos, e definir um plano de tratamento, conforme observação do cenário principal.

[6] Roubo de Wi-Fi preocupa mais de 68 milhões de brasileiros, aponta estudo do dfndr lab. https://www.psafe.com/blog/roubo-de-wi-fi-preocupa-mais-de-68-milhoes-de-brasileiros-aponta-estudo-do-dfndr-lab/

Analisando o cotidiano, a palavra risco passa a ser relacionada a aspectos de natureza física (maior possibilidade de exposição a acidentes), sendo muito utilizada ao se demonstrar o controle nos espaços de trabalho. Nesses locais, existem diversas medidas que são implementadas com o objetivo de averiguar a exposição do trabalhador a ameaças, onde algumas das medidas escolhidas são mais preferíveis em relação a outras. Esse recurso, denominado medida de controle (*HOC-Hierarchy of Controls* - ISO 45001- Sistema de saúde e gestão ocupacional) é um modelo hierárquico voltado a segurança do trabalho, baseando-se numa estrutura geralmente triangular/piramidal onde são tomadas possíveis decisões diante o risco, prezando pelas ações que possuem maior grau de efetividade.

Figura 4 - Modelo de controle de risco HOC



Fonte: https://www.ddsonline.com.br/seguranca/hierarquia-no-controle-de-riscos/ (2020).

Com a implantação da ISO 45001 (Sistema de Gestão de Saúde e Segurança Ocupacional - SGSSO), a utilização da ferramenta HOC entrou na rotina de empreendimentos, onde diversas estratégias foram definidas para mitigar, eliminar ou encontrar riscos, tornando-se uma ferramenta obrigatória para empresas que buscavam criar segurança no ambiente de trabalho (ERPLAN, 2018). Existem diversos modelos HOC, sendo todos construídos nos mesmos princípios básicos de controle e eficiência.[7] A escolha de modelos facilita em

[7] Hierarquia das medidas de controle. visto em: https://www.unifal-mg.edu.br/riscosambientais/node/24

entendimento e visualização mais intuitiva, tornando a tomada de escolhas mais efetivas e organizadas, conforme situação de risco específico.

2.6.1 Escolha de organização hierárquica para proteção de dados sensíveis e benefícios

Levando em consideração a alta demanda de dados sensíveis na saúde, a recomendação principal sugerida para a implementação da segurança dos dados consiste nos requisitos baseados nas normas ISO/ABNT NBR 27001, 27002, estendida conforme as técnicas de segurança da ISO 27701. Esses requisitos são classificados de acordo a escalas de segurança mínimas, prioritárias e avançadas (ver anexo A - categorias do controle de risco conforme ISO/ABNT 27701/27001). Conforme a norma 27001, "4.1 A organização deve determinar as questões internas e externas que são relevantes para o seu propósito e que afetam sua capacidade para alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação", ou seja, é tomada a liberdade de se determinar as escolhas e ordens de segurança de acordo ao cenário e riscos oferecidos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p. 1).

> Como há uma quantidade finita de recursos para implementação de controles de segurança, para o alcance de uma situação de equilíbrio é necessário estabelecer prioridades, identificando quais atividades são essenciais à atuação da organização e até que ponto elas são influenciadas por riscos de segurança. Todas as ações de segurança devem ser prioritariamente guiadas para a preservação da continuidade do desempenho dessas atividades e alcance das metas a elas associadas [...]. Dessa forma, o gestor de segurança precisa encontrar um ponto de equilíbrio entre o ganho no aumento da segurança em comparação com as perdas decorrentes de investimentos em controles e aquelas relacionadas à perda de flexibilidade organizacional (FERNANDES, 2009, p. 14).

Dada a liberdade de escolher passos para seguir na proteção de dados, é interessante pensar em modelos que possam facilitar na tomada de decisão dos dados sensíveis, de tal maneira que essa escolha minimize ou interrompa impactos relacionados a tempo, dinheiro ou manuseio. Tomando como exemplo o modelo HOC, que conforme visto, classifica hierarquicamente as melhores escolhas conforme o impacto, foi escolhida a construção de um modelo de controle de risco para dados sensíveis. Essa iniciativa teve como motivação a organização classificatória e seus benefícios, diante a tomadas de decisão em situações relacionadas às operações dos dados como a manutenção, armazenamento, manipulação e exclusão.

Tabela 3 - Comparativos de um controle de risco organizado e não organizado

	Controle de risco organizado	Tomadas de controle não organizadas
Escolha das medidas de segurança	Decisões mais aplicadas ao risco especifico	Aplicação de medidas não efetivas, gerando operações incorretas sobre as vulnerabilidades, "ocultação" do risco e possivelmente futuras ameaças aos dados.
Custo de adoção de medidas	Melhor avaliação custo-beneficio. Os custos associados às medidas de segurança são comparados com as potenciais perdas que ocorreriam se as ameaças se tornasse realidade.	Não há calculo de impacto, logo pode ocorrer maior custo/prejuizo financeiro para a organização
Aprendizagem	Na tomada organizacional de medidas contra ameaças, não só o setor de TI mas toda a empresa passa a entender os passos de controle, pela facilidade intuitiva	Aplicabilidade menos intuitiva e mais apressada, tornando-se pressionada e dificultando a aprendizagem.
Análise de eventos	A análise de eventos de forma organizada evita esforço desnecessário. Na análise de consequências e impactos, uma vez que, se não forem encontrados quaisquer eventos que poderiam afetar um ativo, não há necessidade de empregar muitos recursos na identificação de consequências e impactos.	Uma análise de eventos desorganizada gera maior custo, já que os ativos não são analisados corretamente, sendo empregadas técnicas muitas vezes redundantes ou ineficientes.

Fonte: A autora (2022).

Considerando o respeito já existente aos dados pessoais no setor médico, o que envolve, como exemplo o sigilo, surge a necessidade do tratamento de dados, o que gera benefícios ao cidadão em termos de confiança e interoperabilidade (CONFEDERAÇÃO NACIONAL DE SAÚDE, 2021). Entende-se que construir um modelo de controle de risco hierárquico passou a ser uma estratégia interessante aos dados sensíveis, já que a organização poderá auxiliar na aceitação, mitigação e redução das ameaças, a partir da abordagem de escolhas classificadas por eficiência e prioridades.

3 GESTÃO E PROTEÇÃO DE DADOS SENSÍVEIS

3.1 História da proteção de dados

O avanço computacional nos anos 70 em países mais desenvolvidos como Alemanha e Estados Unidos foi crucial para impulsionar a criação de normas que pudessem regulamentar a proteção e privacidade dos dados. Conforme Mendes (2020), normas para proteção de dados iniciaram-se em Hesse, Alemanha nos anos 70 (lei de Bundesdatenschutzgesetz), finalizada e implementada em 1978, sendo considerada a primeira lei de proteção de dados do mundo.

Após a implementação Alemã, países como Suécia, Áustria e França passaram a criar suas próprias legislações através das diretrizes sobre proteção da privacidade e fluxo transnacional, publicada pela OECD (*Organization for Economic Cooperation and Development)* e a convenção 108 (primeiro tratado internacional juridicamente vinculativo responsável pelo tratamento da privacidade e proteção de dados) em 1981, organizada pelos países do conselho Europeu.

Dos tratados de proteção de dados, a convenção 108 destacou-se ao estabelecer regras importantes, como a exigência de formas legais na operação dos dados, a atualização nos armazenamentos, o estabelecimento dos direitos e questionamentos do titular sobre o controle dos dados e a garantia de obtenção de cópias e correção em possíveis erros. Países signatários deveriam editar as leis de proteções locais de acordo com a convenção geral (FILHO, 2013).

Entretanto, mesmo com a implantação das diretivas citadas pela convenção 108, o processo não ocorreu de forma ampla, já que algumas leis nacionais isoladas para proteção de dados já existiam em alguns países antes da convenção (FILHO,2013). Além disso, falhas de auto execução e a ausência de termos relacionados aos “adequados” níveis de proteção abriram espaço para que diversos países definissem seus próprios conceitos de proteção de dados pessoais.

A correção da amplitude legislativa seria feita em 1995, através da diretiva 95/46/EC Europeia. A diretiva trouxe maior extensão protetiva, ao estabelecer a exigência do responsável encarregado pela aplicação das leis de proteção e privacidade. Também ampliou o conceito do dado como “qualquer informação relativa à identificação de um titular, como fotos ou registros audiovisuais”. Essa mudança na perspectiva dos dados foi fundamental para a sanção de leis futuras ainda mais especializadas, como a regulamentação geral sobre a proteção de dados.

3.1.1 Regulamentação geral da proteção de dados - RGPD

A regulamentação geral de proteção de dados (GRPD - *General Data Protection Regulation*) consiste em um conjunto de medidas que tem como principal objetivo a proteção

digital em territórios europeus, normatizando a utilização de informações e dados em cenários eletrônicos. A legislação foi adotada em maio de 2016, tendo como exigência a transposição pelos países até maio de 2018.

Uma das principais propostas da RGPD está relacionada à exigência de regulamentação sobre empresas que tratam dados pessoais estabelecidas na União Europeia, independentemente do local de tratamento dos dados. Além disso, é aplicável tanto a empresas que monitoram o comportamento de cidadãos pertencentes a regiões da UE como as estabelecidas de fora da UE que tratam dados pessoais relacionados a ofertas de bens e serviços a pessoas direcionadas ao bloco[8].

No ponto de vista organizacional, a RGPD restringe diretamente as operações de companhias que trabalham de forma direta ou indireta com os dados; A legislação possui alcance global e sem essa adaptação as empresas são consideradas inaptas para manuseio e armazenamento de dados.

> [...] A adoção da GDPR tem grande importância para o mundo corporativo, uma vez que a maioria das empresas trabalha direta ou indiretamente com a utilização de dados virtuais de seus clientes. Isso faz com que a segurança das informações dos consumidores seja vital para as transações feitas por essas companhias. Além disso, a própria operação das companhias muitas vezes acaba se tornando dependente da adequação às normas desta regulamentação, pois, com a padronização global baseada na GDPR, uma empresa que não se enquadrar estará inapta para manusear os dados virtuais dos clientes.
>
> DOCUSIGN. Visto em: https://www.docusign.com.br/blog/gdpr-entenda-o-que-e-o -regulamento-geral-de-protecao-de-dados.

Analisando a RGPD pelo contexto dos dados, a legislação é bem é ampla, com as definições sendo fixadas conforme artigo 4:

> "Dados pessoais são a informação relativa a uma pessoa singular identificada ou identificável, sendo o titular considerado uma pessoa singular que possa ser identificada, direta ou indiretamente, seja por nome, número de identificação, dados localizadores, ou elementos específicos como fisiológicos, genéticos, mentais, culturais e ou sociais. "

No artigo 51, são abordados os critérios relacionados aos tratamentos de dados sensíveis:

- "Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado

[8] Proteção de dados: o que já foi feito na Europa. Visto em: https://conectaja.proteste.org.br/rgpd-o-que -ja-foi-feito-sobre-proteção-de-dados-na-europa/

> que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais".

Apesar da RGPD ser uma lei escrita e regulamentada em território Europeu, a ampla preocupação com as categorias especiais de dados e a importância relacionada a proteção e exportação de dados para fora de regiões da União Europeia ocasionaram a amplitude mundial da lei, tornando-se inspiração aqui no Brasil para a lei geral de proteção de dados - LGPD.

3.2 Histórico de proteção dos dados no Brasil e a lei geral de proteção de dados - LGPD

Assim como os países Europeus, a criação de leis para proteção dos dados passou a ser necessária no Brasil, oriunda do crescimento industrial e computacional. Inicialmente, a Constituição Brasileira de 1988 trouxe alguns pontos referentes à proteção de dados, como a garantia da intimidade, imagem e honra, assegurando o direito à indenização pela inviolabilidade. Além desta, a criação do código de defesa ao consumidor também ajudou na evolução das proteções relacionadas às informações sobre cadastros e banco de dados (MENDES, 2020).

Para a regularização da internet do país foi decretado em 2013 o Marco civil, lei que possui como princípios a proteção da privacidade de dados e a exigência de consentimento livre e expresso ao usuário, assegurando a inviolabilidade e sigilo do fluxo de comunicações privadas armazenadas, salvo ordem judicial[9]. O marco civil reforça a relação da proporcionalidade e razoabilidade, já que, conforme Alencar (2021), ocorre o conflito entre os direitos relacionados à privacidade e à liberdade de expressão.

Alguns dos princípios do marco civil são:

- Garantia da liberdade de expressão, manifestação de pensamento e comunicação.
- Proteção da privacidade.
- Inviolabilidade da intimidade e vida privada.
- O não fornecimento a terceiros dos dados pessoais, salvo em consentimento livre ou em hipóteses de lei.
- O provedor de serviços só será responsabilizado se, caso exista ordem judicial específica o mesmo não tomar providências para tornar indisponível o conteúdo indicado como infringente.

[9] Marco Civil da Internet. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet.

Assim como no marco civil e sendo influenciada pela GRPD, a LGPD (lei geral de proteção de dados), sancionada em agosto de 2018, foi redigida com o objetivo de determinar regras nas quais as organizações deveriam seguir para tratamento de dados, reforçando direitos fundamentais da privacidade. Comparada a RGPD, Pinheiro (2020) define que a LGPD é menos extensa, o que pode ocasionar interpretações ambíguas e pontos de insegurança jurídica, porém possui pontos vitais para a proteção, acesso dos titulares e dados sensíveis.

Em relação aos dados, tanto os pessoais quanto os sensíveis, considera-se conforme artigo 5°, inciso I e II:

- **I - Dado pessoal:** Informação relacionada a pessoa natural identificada ou identificável;
- **II - Dado pessoal sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Em relação ao tratamento, entende-se que a cautela deve ser maior em relação aos dados sensíveis, já que riscos de segurança podem ocasionar consequências danosas à liberdade e aos direitos dos usuários. O artigo 11 da LGPD expõe a tratativa relacionada aos dados sensíveis que estão relacionadas a:

- I - Livre consentimento
- II - Sem consentimento, para casos onde exista:
    1. Cumprimento de obrigação legal e tratamento compartilhado de dados necessários à execução pela administração pública.
    2. Realização de estudos por órgão de pesquisa.
    3. Exercício regular de direitos, inclusive em contrato, processo judicial, administrativo e arbitral.
    4. Proteção da vida ou da incolumidade física do titular ou de terceiros.
    5. Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.
    6. Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Conforme Atheniense (2021), o setor de saúde lida com dados pessoais classificados como “sensíveis” pela LGPD, e, portanto, clínicas, hospitais e profissionais estão mais expostos a possíveis vazamentos e processos relacionados aos pacientes e outros titulares de dados, além

de sanções por órgãos fiscalizadores. Portanto é necessário seguir as adequações e os cuidados impostos pela LGPD para proteção dos dados sensíveis como:

- Adotar medidas protetivas com os dados sensíveis, com políticas de segurança da informação e políticas de segurança documentais.
- Ter cuidado ao utilizar ferramentas de baixa segurança para operação de dados sensíveis, como planilhas, ferramentas de comunicação pessoal, mensageiros instantâneos e redes sociais.
- Consultórios e médicos autônomos também têm a mesma responsabilidade de cumprimento das regras da LGPD, assim como grandes organizações.
- Serviços de terceiros também precisam ter as políticas de segurança revisadas (compartilhamento de dados com planos de saúde e convênios).

3.3 Gestão documental e operações de dados

Sendo importantíssima para o gerenciamento de informações e dados, a gestão documental é caracterizada como o conjunto de métodos responsáveis pelos procedimentos de armazenamento, manipulação, produção e conservação dos documentos em uma organização, permitindo o bom funcionamento dos setores através da atuação estratégica.

Com o crescimento tecnológico, a conversão de informações físicas para digitais e a utilização de serviços em nuvem para armazenamento tornou-se iminente. Leis como a 12.682/2012 (elaboração e o arquivamento de documentos em meios eletromagnéticos) regulamentaram a operação de documentos públicos, porém devido a diversos vetos referentes ao comparativo entre o valor de documentos digitais e físicos houve a exigência de implementações que trouxessem legitimidade e segurança dos documentos digitais.

Entretanto, ainda que o avanço tecnológico tenha oferecido a possibilidade da conversão dos documentos, as organizações ainda optam por utilizar documentos físicos. As vantagens dessa utilização estão na independência de acesso, na sensação de segurança e no cumprimento legislativo, onde registros impressos são escolhidos devido a não existir regulamentações totais sobre documentos digitais. As desvantagens estão relacionadas a vida útil, o espaço, o risco de perda e custos aparentes, como papéis, impressão ou pastas.

Tanto as opções digitais quanto físicas oferecem vantagens e desvantagens, bastando a cada organização a escolha de acordo com suas demandas.

> Ambas as formas de documentações, tanto físicas quanto como digitais contam com vantagens e desvantagens, portanto, a escolha deve considerar as características e necessidades do seu negócio. [...]. Nesse caso, os arquivos físicos que devem ser

> mantidos são arquivados em um espaço seguro, protegido contra intempéries. Enquanto isso, as cópias digitais são disponibilizadas para que a equipe utilize no dia a dia.[...]. Dessa maneira, a empresa consegue organizar os arquivos, facilitar o acesso, aumentar a segurança e otimizar os processos internos. Como consequência, é possível ter mais produtividade e reduzir os custos relacionados, obtendo melhores resultados na gestão.
>
> Prado Chaves. Visto em https://www.pradochaves.com.br/documentos-digitais-x-fisicos -quais-as-vantagens-e-desvantagens/

Tabela 4 - Características dos documentos físicos e digitais

Características	**Documentos físicos**	**Documentos Digitais**
"Sensação" de segurança (Confiança)	X	Ainda há resistência nos documentos digitais devido às implantações recentes.
Acesso independente a tecnologia	X	
Cumprimento Legislacional	X	Sim, apesar da resistência inicial devido às regulamentações de documentos digitais
Vida útil ampla		X
Redução de espaço utilizado para armazenamento		X
Riscos ocasionados por perda e dano	X	
Custos altos de manutenção	X	
Sustentabilidade		X
Aumento de produtividade na localização e manipulação		X

Fonte: A autora (2022).

Legislações como a da RGPD e LGPD trouxeram a discussão de dados além do critério digital, ou seja, a responsabilidade de proteção é igualitária para diversos formatos. Como exemplo, a LGPD enfatiza o armazenamento dos dados, reforçando que estes só podem ser mantidos enquanto possuírem relevância na organização. Essa solicitação acaba reforçando a necessidade da implantação de ciclos de tempo através da teoria das três idades[10], que deve ser implementada de acordo com a relevância e utilização de cada documento.

[10] A teoria das três idades é a responsável por definir valores temporais dos documentos, sendo fundamental para aplicação da permanência, exclusão e arquivamento. A teoria utiliza como princípio de aplicabilidade a tabela de temporalidade e o código de classificação dos documentos (ENAP, 2015).

Tabela 5 - Tabela das três idades do ciclo documental

1ª IDADE	**ARQUIVO CORRENTE**	Conjunto de documentos vinculados aos **fins imediatos** para os quais foram produzidos ou recebidos e que, mesmo cessada sua tramitação, conservam-se **junto aos órgãos produtores** em razão da frequência com que são consultados.
2ª IDADE	**ARQUIVO INTERMEDIÁRIO**	Conjunto de documentos originários de arquivos correntes, com **uso pouco frequente**, que aguardam sua destinação final.
3ª IDADE	**ARQUIVO PERMANENTE**	Conjunto de documentos preservados em **caráter definitivo**, em função do seu valor, como prova, garantia de direitos ou fonte de pesquisa.

Fonte: ENAP (2015)

A gestão de documentos físicos e digitais é primordial. Dependendo do número das atividades realizadas, o acúmulo e o acesso a documentos pode se tornar problemático. Conforme Bernardes e Delatorre (2008), a falta de políticas relacionadas à gestão documental como a ausência de normas, métodos e procedimentos de protocolização gera o acúmulo desordenado de documentos, dificultando o acesso a informações. Isso mostra que são necessários planos envolvendo processos de classificação e temporalidade.

A disposição complexa de documentos, assim como a falta de organização e gestão no acesso contribuem para ocorrências relacionadas a falhas de segurança em dados pessoais e sensíveis, amplamente utilizados no cenário médico e hospitalar (falhas relacionadas à segurança em documentos físicos e digitais serão melhor abordadas no Cap. 4).

3.4 Relação das Normas ISO 27001, 27701 e 27002 com a proteção de dados sensíveis

As normas ISO são documentos escritos que têm como objetivo o estabelecimento e padronização de procedimentos aplicados a produtos, setores e organizações. São escritas pela *International Organization for Standardization*, uma organização Sueca, sendo representada no Brasil pela Associação Brasileira de Normas Técnicas (ABNT), entidade privada e sem fins lucrativos.

A ISO 27001 (Sistemas de gestão de segurança da informação), 27701 (Técnicas de segurança - extensão da ISO/IEC 27001), 27002 (gestão da privacidade da informação) e 27002 (Guia de Boas práticas para controles de segurança da informação) abrangem formas de estabelecer processos para a segurança da informação em organizações. Todas as ISOS citadas

não são direcionadas exclusivamente aos dados sensíveis, porém possuem abordagens e normas de controle importantes para o gerenciamento das informações e dados gerais.

3.4.1 ISO 27001

A ISO 27001 é uma norma internacional pertencente à família 27000. Tem como objetivo instruir sobre implementações relacionadas à gestão com foco em segurança da informação. A implantação da norma em ambientes organizacionais tornou-se necessária devido a incidentes e possíveis violações de segurança informacionais. Dividida em 11 seções e anexo A (Segunda versão, 2013), as seções 0 a 3 são introdutórias, 4 a 10 obrigatórias e o anexo A com listas detalhadas dos controles para tratamento de risco:

- **0, 1, 2 e 3 (introdução):** Estabelece a introdução, referências normativas, termos e definições iniciais. Não são obrigatórias para a implantação.
- **4 a 10 (entendimento da organização, liderança, planejamento, apoio, operação, avaliação de desempenho e melhorias):** Tratam dos processos obrigatórios que devem ser implantados na organização para segurança da informação, como planejamento e responsabilidades, lideranças que irão administrar os dados, conscientização, tratamento de risco, comunicações de controles e melhorias na gestão de segurança.
- **Anexo A:** As “salvaguardas” da ISO 27001, que contém normas de controle detalhadas, com o intuito de garantir que nenhum controle necessário seja omitido.

No cenário médico (ou em outro possível cenário que manipule dados sensíveis), ao se adotar as diretrizes da ISO 27001 para implantação de um sistema de gestão de informação, são estabelecidos os seguintes pontos:

- **Seção 4 - Sistema de gestão da segurança da informação:** A organização deve estabelecer, implementar, manter e continuamente melhorar um sistema de gestão da segurança da informação, de acordo com os requisitos desta seção, não esquecendo dos princípios críticos de segurança que são a confidencialidade, integridade e disponibilidade.
- **Seção 5 - Liderança e comprometimento:** A alta direção deve avaliar a compatibilidade da política de gestão com a estratégia da organização, estabelecendo autoridades responsáveis para a proteção dos dados, comunicando os colaboradores sobre a importância da implantação e cuidados que podem ser tomados, documentando políticas, revisando os resultados do sistema de gestão e apoiando aqueles que contribuam para sua eficácia.

- **Seção 6 - Planejamento:** Através de determinação interna e externa, a organização deve avaliar fatores relevantes que podem ocasionar riscos aos dados. Nesta seção, entrará a análise de risco, e serão planejadas as ações para prevenir ou reduzir efeitos que influenciam na gestão de proteção da informação.
- **Seção 7 - Estabelecimento de recursos:** Onde a organização será responsável pelo estabelecimento de recursos para a implantação da gestão de segurança (não somente recursos financeiros, mas todos os recursos responsáveis por melhorias na implantação, como informações documentadas, comunicações, avaliações de competência daqueles que operam os dados, conscientização sobre a proteção e fornecimento de treinamento necessário.
- **Seção 8 - Operação:** Onde a organização deve implementar a avaliação e controles de processos, conforme avaliados no planejamento da seção 6.
- **Seção 9 - Avaliando o desempenho:** Na penúltima seção, será avaliado os fatores da implantação, como a eficácia, se os métodos escolhidos cobrem todo o cenário existente e auditorias.
- **Seção 10 - Melhorias:** Onde será observada a conformidade da implantação e gestão, onde serão feitas ações corretivas ao se analisar a conformidade da implementação. Caso haja algo em não conformidade, ações corretivas serão aplicadas para controlar e tratar falhas, melhorar a pertinência e eficácia do sistema de gestão (Para exemplo de aplicabilidade das normas ISO 27001 a um cenário médico ver Apêndice A).

A ISO 27001 cita os dados sensíveis brevemente em dois momentos: no Anexo A.11.1.1 (Perímetro de segurança física) e A.11.2.7 (Reutilização e ou descarte seguro de equipamentos):

- A.11.1.1: Perímetros de segurança devem ser definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis.
- A.11.2.7: Equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.

Apesar da ISO 27001 abordar os dados sensíveis de maneira rápida, o ciclo de implantação proposto é totalmente abrangente ao cenário dos dados sensíveis, tornando-se uma excelente e importante ferramenta para áreas médicas e outros ambientes que tratam destes dados.

4 RISCOS DE SEGURANÇA RELACIONADOS AOS DADOS SENSÍVEIS

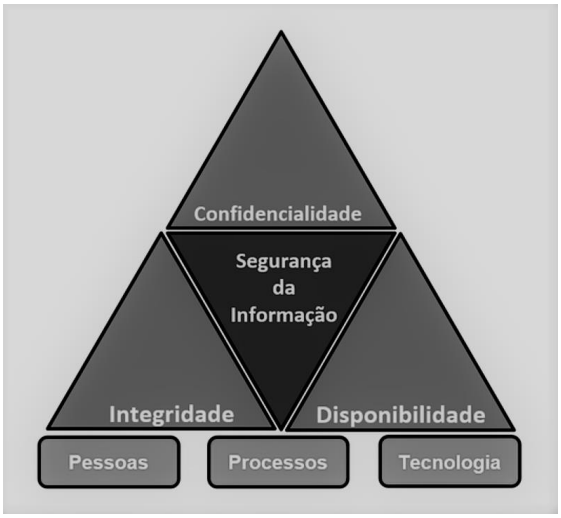
No presente capítulo serão abordados os riscos e ameaças relacionadas aos dados sensíveis, bem como os processos de segurança, análise de fatores humanos e gestão documental.

4.1 Tríade CIA

O processo de segurança dos dados físicos e digitais envolve a implantação do sistema de gestão, que deve conter técnicas responsáveis para proteger os processos e tratamentos, assim como a análise de risco que tem o objetivo de averiguar e conduzir para a tomada de decisões que melhor protejam os dados.

Independente dos dados serem ou não sensíveis, para a sua proteção é importante a priorização dos princípios fundamentais da segurança (Disponibilidade, Integridade e Confidencialidade). Conforme HINTZBERGEN et al (2018, pág. 20), “um programa de segurança pode ter diversos objetivos grandes e pequenos, mas os princípios mais importantes são os fundamentais de segurança dos dados”. Ou seja, independente das diferenças entre análises de risco e objetivos adotados, todas as organizações devem prezar pela execução do ciclo CIA (Confidentiality, Integrity and Availability).

Figura 5 - Tríade CIA



Fonte: blog.matheustech.com.br/post/seguranca-da-informacao (2020)

A confidencialidade trata da restrição de acesso, ou seja, define quem (usuário, processo ou organização) pode ter acesso ou não a determinado dado. O principal objetivo é garantir que os acessos não sejam disponibilizados sem autorização. A integridade visa a consistência dos dados, ou seja, preza-se pela preservação. Por último, a disponibilidade é caracterizada pela acessibilidade, ou seja, um dado deve ser acessado quando necessário, sem falhas ou interrupções.

Um dado que é modificado sem permissão é um exemplo de uma violação contra a integridade, assim como a divulgação/exposição de algum dado sem autorização é uma violação contra a confidencialidade.

Além da tríade CIA, entender as definições e conceitos de segurança definidos na ISO 27000 também ajudam na análise e combinação de controles para prezar pela segurança sensível. Cada organização deve construir seu próprio nível de segurança, já que os objetivos na avaliação variam de cada cenário.

4.2 Risco, vulnerabilidade e ameaças

Quando uma organização pretende implantar diretrizes que visem a proteção dos dados, entender as definições e conceitos de segurança facilitam no entendimento e na visão geral do SGSI (Sistemas de Gerenciamento de Segurança da Informação). Compreender a diferença entre os termos é crucial para realizar a avaliação de risco e possíveis tomadas de decisão frente a situações de ameaças aos dados sensíveis.

Como a principal ação é tentar evitar qualquer situação que cause prejuízo aos dados, é importante determinar o risco. Uma fórmula utilizada para demonstrar a determinação do risco é:

$$A + AM + V = R$$

Onde A = ativo, AM = ameaça, V= vulnerabilidade e R= risco[11]. Essa fórmula enfatiza que embora a ameaça exista, se a vulnerabilidade for nula, o risco será mínimo. O mesmo vale para a vulnerabilidade.

A família ISO 27000 dispõe no capítulo 3 de termos e definições gerais dos SGSI, aplicáveis a todos os tipos e tamanhos de organizações. Iremos nos concentrar nas três definições mais conhecidas na segurança da informação: risco, vulnerabilidade e ameaça:

[11] Ameaça, vulnerabilidade, risco – Sopa de letrinhas. Visto em: https://www.itfacil.com.br/ameaca-vulnerabilidade-risco-sopa-de-letrinhas.

- **Risco:** O risco é o princípio da incerteza, ou seja, um evento que não era previsto de se acontecer. Na segurança da informação é comum enfatizar o risco apenas de caráter negativo, porém o resultado do evento pode ser neutro ou positivo.

A análise de risco concentra-se justamente no potencial de ameaças que podem atingir os ativos. Ou seja, identifica-se o possível evento que cause potenciais falhas ao SGSI e a todo o projeto implantado na organização.

Tabela 6 - Ações e riscos no ambiente sensível

	Ação	Exemplo	Risco
Cenário físico	Alocação incorreta os dados e informações sensíveis	Uma ficha medica exposta na mesa	Vazamento de dados Corrupção de dados Quebra dos principios CIA (confidencialidade, disponibilidade e integridade)
	Reaproveitamento da informação	Utilização de documentos sensíveis como rascunho	
	Eliminação incorreta da documentação	Eliminar documentos sem torna-los inelegíveis	
	Acesso facilitado ao local	Salas de arquivos sensiveis facilmente acessíveis	
Cenário digital	Compartilhamento indevido de informações entre mensageiros instantâneos	Fotos de pacientes compartilhadas em grupos pessoais	
	SGSI incompleto ou falho (acesso facilitado, ausencia de logs em modificações de documentos	Login de um SGSI médico com senhas padrões, ou sem senhas Alteração de documento sem autorização/ verificação de logs	
	Rede sem proteção	Porta de um firewall facilmente acessivel	

Fonte: A autora (2022)

Deve-se levar em conta que ações não propositais também podem ocasionar riscos. Fenômenos da natureza ou ações humanas não intencionais (por falta de treinamento em procedimentos) são ações que geram eventos inesperados nos ativos, de forma neutra, ou até mesmo de forma negativa.

- **Vulnerabilidade:** A vulnerabilidade é caracterizada como a fragilidade que a organização possui nos ativos. Essas fraquezas geralmente são buscadas pelos atacantes com o objetivo de prejudicar, danificar ou obter acesso aos ativos. Uma sala contendo arquivos sensíveis que possui acesso facilitado é uma sala vulnerável, assim como uma porta facilmente explorável no firewall.

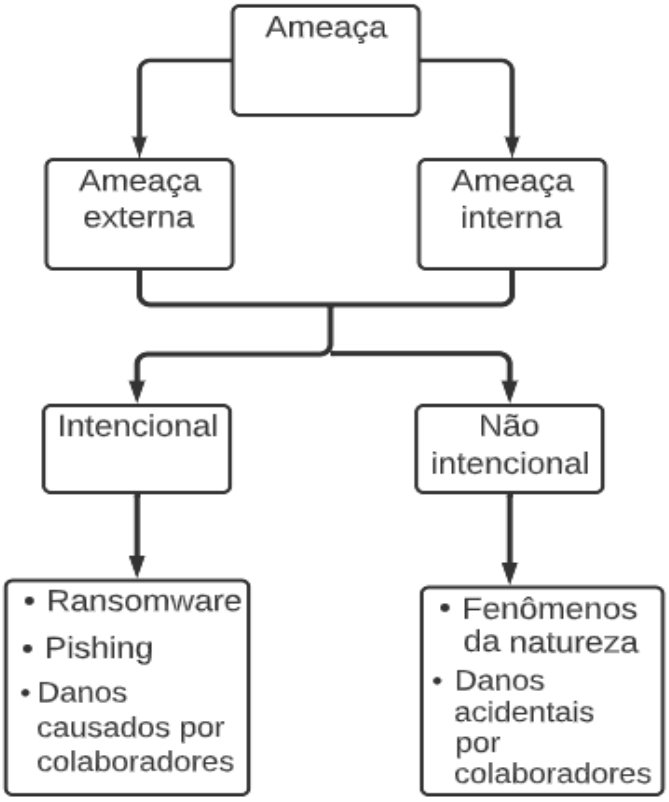
- **Ameaça:** A ameaça é um evento ocasionado com o intuito de prejudicar o ativo. Conforme a ISO 27000 (cap. 3), a ameaça é “uma causa potencial de um incidente indesejado que pode ocasionar danos a um sistema ou organização”. Um ataque a um sistema de arquivo sensível para obter informações, ou mesmo destruí-las é um exemplo

de ameaça. Funcionários cometendo erros não intencionais como apagar arquivos importantes sem permissão, inserir um pen drive com vírus, ou acessar um *e-mail* com *phishing* também são tipos de ameaças.

Ameaças podem variar de acordo a cada país, nível de desenvolvimento e uso da internet (HINTZBERGEN et al., 2018), porém a ameaça necessita de uma fragilidade (vulnerabilidade) para poder agir dentro da organização.

Na definição da análise de risco, as ameaças são listadas de acordo com a sua progressão de dano aos dados e para isso devem ser considerados diversos cenários de ameaça, tanto físicos quanto naturais. As ameaças podem ser divididas em ameaças intencionais e não intencionais, assim como ameaças naturais.

Figura 6 - Diagrama de ameaças



Fonte: A autora (2022)

4.3 Ameaças intencionais e não intencionais aos dados sensíveis

A ameaça intencional é aquela que tem como característica a ação deliberada de prejudicar o ativo. Geralmente os ataques a ativos mais conhecidos são os relacionados a processos intrusos externos, disseminados por *hackers*, apesar que o processo também possa

acontecer de maneira interna por colaboradores da empresa. Já as não intencionais são aquelas ocasionadas pelo descuido, falta de preparo dos colaboradores e políticas falhas de acesso a dados e informações.

Internamente ou externamente, ameaças trazem transtorno, danificando e expondo dados e informações importantes. Mensurar o valor do dado é um processo variável, já que fica difícil saber o valor específico de uma informação, sensível ou não. Porém numa situação de vazamento e exposição, o dado passa a apresentar um valor altíssimo, o que pode gerar complicações para a reputação de uma organização.

4.3.1 Phishing

O *phishing* é uma técnica ilegal onde se tentam enganar usuários para a coleta de informações. Os usuários recebem e-mails ou mensagens (que se passam por pessoas ou organizações conhecidas), induzindo o usuário a acessar links e executar ações (isca). Ao acessar, o usuário se depara com websites legítimos, que incentivam o mesmo a efetuar *logins* e fornecer informações pessoais. Caso forneça, os atacantes obtêm as informações de acesso, como senhas ou outras informações. É uma ameaça intencional.

Diferente de outras ameaças, o *phishing* parte da ideia de enganar a confiabilidade humana (engenharia social). Por tentar utilizar a ideia da persuasão, ataques de *phishing* são difíceis de serem combatidos.

Figura 7 - Exemplo de *Phishing* por e-mail

Fonte: www.lumiun.com/blog/como-funciona-o-golpe-de-e-mail-falso/(2020)

É importante para a organização reconhecer algumas características de *phishing* para poder comunicar aos colaboradores a evitar possíveis ataques:

- Suspeitar do remetente, principalmente se estiver relacionando a mensagem ou cópia de e-mail a grupos e unidades desconhecidas.
- Mensagens que gerem pânico ou que possuam tom de urgência, induzindo o usuário a concretizar uma ação o mais rápido possível.
- Mensagens com anexos desconhecidos, geralmente se passando por conhecidos, anexos simbolizando fotos pessoais, fotos de celebrações, ou até mesmo documentos de trabalho.
- Mensagens com links integrados "apagados" (URL de natureza desconhecida).
- E mails e websites familiares com erros de ortografia. É importante acessar websites com URL segura HTTPS (*Hyper Text Transfer Protocol Secure).*

> Diferente de outros tipos de ameaças online, o *phishing* não requer um conhecimento técnico muito sofisticado. Na verdade, segundo Adam Kujawa, diretor do Malwarebytes Labs, "*Phishing* é o tipo mais simples de ciberataque e, ao mesmo tempo, o mais perigoso e eficiente porque ele ataca o computador mais vulnerável e poderoso do planeta: a mente humana." Os "*phishers"* não tentam explorar uma vulnerabilidade técnica do sistema operacional de seu dispositivo — eles usam a "engenharia social".
>
> MALWAREBYTES. *Phishing*. Visto em: https://br.malwarebytes.com/phishing/.

4.3.2 Ransomware

O *ransomware* é um código malicioso que realiza a criptografia dos dados (torna-os inelegíveis para quem não tem acesso a uma chave ou recurso específico) e exige pagamento para que se tenha novamente o acesso. A ideia é baseada no "sequestro", onde ocorre o bloqueio no acesso, com a liberação sendo efetivada mediante pagamento (extorsão). O pagamento geralmente é exigido via bitcoins (já que na transação de moedas virtuais os dados não são compartilhados, tornando o caminho de operação bancária difícil de ser investigado).

Em formas de extorsão, o ransomware caracteriza-se de duas formas distintas, onde a primeira pode ser baseada em criptografia parcial/cripto, que não permite ao usuário o acesso aos seus arquivos, e a criptografia total/locker, que inviabiliza o acesso a todo o sistema. Conforme LISKA (pagina/ cap. 1), ameaças como as oferecidas pelo *ransomware* não estão limitadas a territórios e sistemas específicos, vindo a se modificar apenas quanto ao tipo de método de comprometimento de arquivos/máquinas, assim como há variações em tipo de extorsão.

Ransomwares geram grandes prejuízos a organizações, independente se os dados operados são ou não sensíveis. Algumas vulnerabilidades são fatores cruciais para possíveis ataques a organizações, como:

- **Dispositivos desatualizados, dispositivos sem antivírus com versões antigas e sistemas operacionais com suporte finalizado:** Softwares necessários para proteção de dados, assim como sistemas operacionais necessitam de suporte oficial, sendo atualizados e trocados caso seja encerrado o suporte.
- ***E-mails* e anexos suspeitos, fontes de download irregulares, conexão de pen drives improcedentes:** Evitar abrir *e-mails* maliciosos, anexos suspeitos, e utilizar ferramentas para detecção de spam. Conexões de pen drivers precisam ser cautelosas, assim como downloads de arquivos em endereços sem procedências.
- **Backup inexistente ou rotinas de backup incompletas:** A falta de backup dificulta a recuperação em caso de possíveis ataques.
- **Falta de políticas de segurança e restrições na organização:** A organização que não possui políticas de proteção de dados torna-se mais vulnerável a ataques. Além disso, a implantação de uma política sem a divulgação e convocação de todos além dos setores de TI também é ineficiente. É necessária a comunicação das políticas e descrição das restrições necessárias a todos os colaboradores.

Figura 8 - Ransomware Petya

Fonte: www.avast.com/pt-br/c-petya (2019)

4.3.3 Risco humano e engenharia social

No contexto de segurança da informação, a engenharia social está relacionada à manipulação psicológica, onde tenta-se enganar e influenciar o usuário para que o mesmo realize alguma ação que desproteja ou divulgue dados e informações. Essa ação pode ser para diversos objetivos, tratando-se de um mecanismo prejudicial e intencional para os ativos.

Além da engenharia social e ameaças externas, fatores propriamente relacionados a ameaças internas e comportamento humano podem ser ainda mais danosos a proteção dos dados. Um colaborador que esteja insatisfeito com a organização ou que tenha sido influenciado por terceiros pode se apropriar dos ativos e divulgá-los, seja para obter lucro ou para prejudicar os dados (fins vingativos ou lucrativos)

Anteriormente vimos que ameaças como o *phishing* aproveitam-se da confiança do usuário para tentar propor a execução de ações com o objetivo de obter ou inutilizar o ativo. O *phishing* é considerado uma ameaça externa que se beneficia da engenharia social para obter proveito. Assim como ele, outros tipos de ameaças externas que exploram a engenharia social também são conhecidos, tais como:

- ***Smishing:*** também sendo uma técnica de *phishing*, mas explorando as mensagens SMS.
- ***Quid pro quo:*** Do latim" tomar uma coisa por outra", induz o usuário a acreditar em um problema, (como uma invasão por vírus) para fazer com que o mesmo baixe uma ferramenta ou forneça algum acesso para resolvê-lo.
- ***Trashing:*** Envolve a busca de informação e dados através da exploração do lixo organizacional (ver proteção de documentos e gestão documental).
- ***Tailgating:*** Envolve o acesso de pessoas não autorizadas a ambientes da organização.

Conforme seção 7 da ISO 27001, a organização deverá estabelecer recursos para a gestão de segurança da informação, tais como a comunicação entre colaboradores. As medidas devem ser orientadas pela organização para os colaboradores com o objetivo de proteger os ativos, como autorização de acesso a locais onde se encontram dados, eliminação correta de lixo organizacional, orientação sobre acesso de *e-mails* e *logins.*

4.3.4 Ameaças naturais e ameaças não intencionais

Ao se abordar a segurança de dados, as organizações investem em políticas de proteções de segurança da informação voltadas exclusivamente as ameaças intencionais, mais

precisamente as externas, porém ameaças involuntárias oferecem grande risco às organizações, podendo gerar impactos negativos aos dados. Classificadas pela grande imprevisibilidade, as ameaças não intencionais muitas das vezes ocorrem por negligência e descuido com as políticas de proteção de dados dentro da organização.

As ameaças naturais, por sua vez, são os fenômenos da natureza que podem ocasionar impactos aos ativos. Podem ser inundações, tornados, tempestades, incêndios ou outros fatores.

Uma sala de servidores centrais pode ser danificada com descargas elétricas. O mesmo vale para uma sala de arquivos físicos que pode sofrer com um evento de incêndio. As ameaças naturais são difíceis de serem previstas, porém existem passos que podem corrigir ou minimizar os danos sofridos, como a adoção de seguros para proteger os ativos, auxílios de caráter governamentais e planos de contingências.

Já as ameaças não intencionais são processos advindos boa parte das vezes por colaboradores desatentos ou que agem com negligência as políticas de proteção de dados. Essas ameaças podem atacar tanto de forma branda os ativos físicos e digitais, como podem oferecer grande potencial de risco, inativando ou expondo os dados.

Alguns fatores aumentam significativamente o risco de ameaças involuntárias como:

- **Acessos facilitados ou liberação de controle desnecessário:** Liberações de acesso total a colaboradores aumentam as chances de acontecer imprevistos de segurança aos dados. É necessário informar a todos sobre o risco iminente em grandes privilégios dos sistemas internos e somente fornecê-los de acordo ao cargo e necessidade da função.
- **Mapeamentos de redes irregulares e dispositivos desconhecidos:** abrange o acesso indiscriminado de colaboradores a rede interna da empresa, o que pode causar também ataques e vazamentos.
- **Configurações incorretas em dispositivos de rede e falta de conhecimento dos operadores de rede.**
- **Encaminhamento de e-mails confidenciais sem autorização**.
- **Desconsideração com normas de segurança:** nesse ponto, mais uma vez entra o comportamento humano. O colaborador pode estar ignorando as regras porque simplesmente acredita que não há riscos para a organização ou porque as desconhece.

4.4 Proteção de documentos e gestão documental

Em geral, as organizações produzem grandes quantidades de documentos, sejam para armazenamento de informações ou para tomada de decisões importantes. Muitos desses

documentos possuem valores confidenciais altos e por isso é importante manipulá-los de forma segura. Entender o valor dos dados em cada documentação é importante para se tomar medidas de proteção.

A gestão documental vem como forma de preservar e trazer a segurança através de procedimentos que definem os fluxos de documentos e arquivos, como formas corretas de armazenamento, temporalidade e processos de eliminação. A LGPD enfatiza o armazenamento dos dados, reforçando que estes só podem ser mantidos enquanto possuírem relevância. Essa solicitação acaba reforçando a necessidade da implantação de ciclos de tempo através da teoria das três idades[12], que deve ser implementada de acordo com a relevância e utilização de cada documento.

Usualmente em ambientes médicos, a manipulação de dados sensíveis, tanto em sistemas de gestão como em processos de documentos físicos é alta. Analisando um cenário de atividades de saúde, as manipulações dos dados teriam fatores de risco importantes para serem analisados, como:

- **Recepção e abordagem ao usuário:** ao se abordar o usuário são coletados os dados. Onde os dados serão armazenados? Se forem armazenados de forma física, como será disposta a organização a esse documento? Mesmo físico, é importante saber quem irá manusear, visualizar e ficar sob tutela dos documentos.
- **Setores de arquivo:** onde serão dispostos os documentos, e como ficará o processo, conforme visto no cap. 3, de ciclos de tempo (teoria das três idades)? Quem deve ter acesso a sala dos arquivos? A teoria dos ciclos de três idades está sendo respeitada? Como está sendo a implantação?
- **Divulgação das informações e reutilização:** Com a expansão de recursos tecnológicos, novas abordagens como a telemedicina e a utilização de aplicativos facilitou a abordagem médica/paciente, permitindo melhor acessibilidade a mecanismos de saúde. Porém, como será feita a utilização dos recursos? Quem verá a informação médica, e quais serão as finalidades? Documentos, informações sensíveis e com conteúdo possivelmente confidencial não poderão ser utilizados como rascunho, divulgados sem autorização em plataformas e mensageiros instantâneos.

[12] A teoria das três idades é a responsável por definir valores temporais dos documentos, sendo fundamental para aplicação da permanência, exclusão e arquivamento. A teoria utiliza como princípio de aplicabilidade a tabela de temporalidade e o código de classificação dos documentos (ENAP, 2015).

- **Eliminação de documentação:** A eliminação de documentos deve levar em conta a teoria das três idades. O tratamento de dados deve equivaler a todo o ciclo de vida documental, ou seja, a eliminação também é crucial. Deve ser utilizado o ciclo vital documental; se o documento não é mais constantemente usado ele passa para a segunda idade, a intermediaria, podendo partir para eliminação após análise.

É importante frisar que a LGPD não possui procedimentos sobre a forma que os documentos devem ser eliminados. Um entendimento que se tem sobre a eliminação é que o principal objetivo é a descaracterização documental, devendo ocorrer pela fragmentação manual ou mecânica, desmagnetização ou reformatação, garantindo que não haja reversão nas características dos documentos (UNIFESSPA, 2018).

Com a finalização dos possíveis riscos para os dados sensíveis, é importante pensar em medidas para garantir a segurança. No capítulo cinco serão abordados os passos seguidos para a proteção dos dados sensíveis, entre eles a construção do controle hierárquico.

5 ESTUDO DE CASO

No presente capítulo, para análise de tratamentos e movimentações dos dados sensíveis será apresentada uma empresa (fictícia). Após isso, serão mostradas possíveis situações que representem vulnerabilidades e a partir destas, a análise de risco será definida.

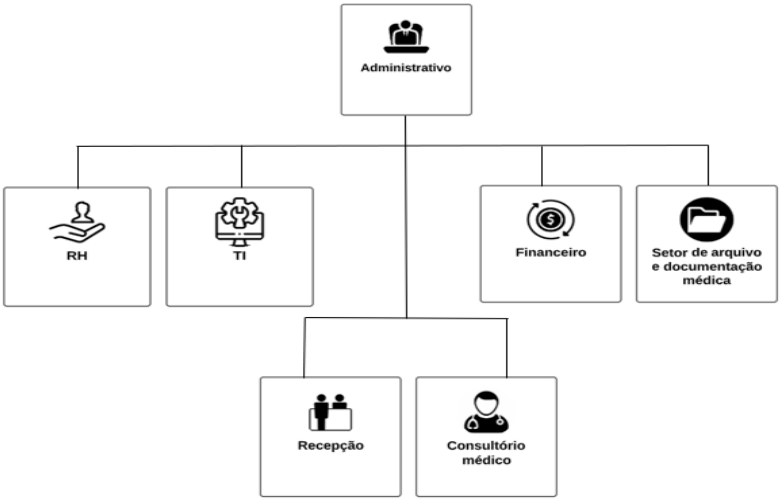
Para a representação do cenário desse capitulo, serão utilizados como escopo os anexos da ISO 27001 (anexo A - Referência aos controles e objetivos de controles), 27005 (anexo D - Vulnerabilidades e métodos de avaliação de vulnerabilidades), bem como as seções formativas. O ciclo de dados médicos, bem como a análise de risco também serão construídos tomando como base o código de boas práticas - proteção de dados para prestadores privados em saúde e a ISO 45001(Capitulo 8: Operação).

Com a análise de risco construída, o controle de risco será demonstrado, conforme cenário fictício escolhido.

5.1 Apresentação da empresa fictícia e cenário principal

A empresa Med&clinic tem como objetivo serviços médicos. Sendo uma empresa de médio porte, é composta de 23 colaboradores, divididos em setores específicos: recepção, salas de exames, financeiro, RH, setor de arquivo e documentação médica, setor de TI e setor administrativo. Atualmente a empresa atende em torno de 100 a 120 clientes diários, tendo como foco principal a realização de exames admissionais. A figura abaixo apresenta o organograma da empresa:

Figura 9 - Organograma - Empresa Med&Clinic

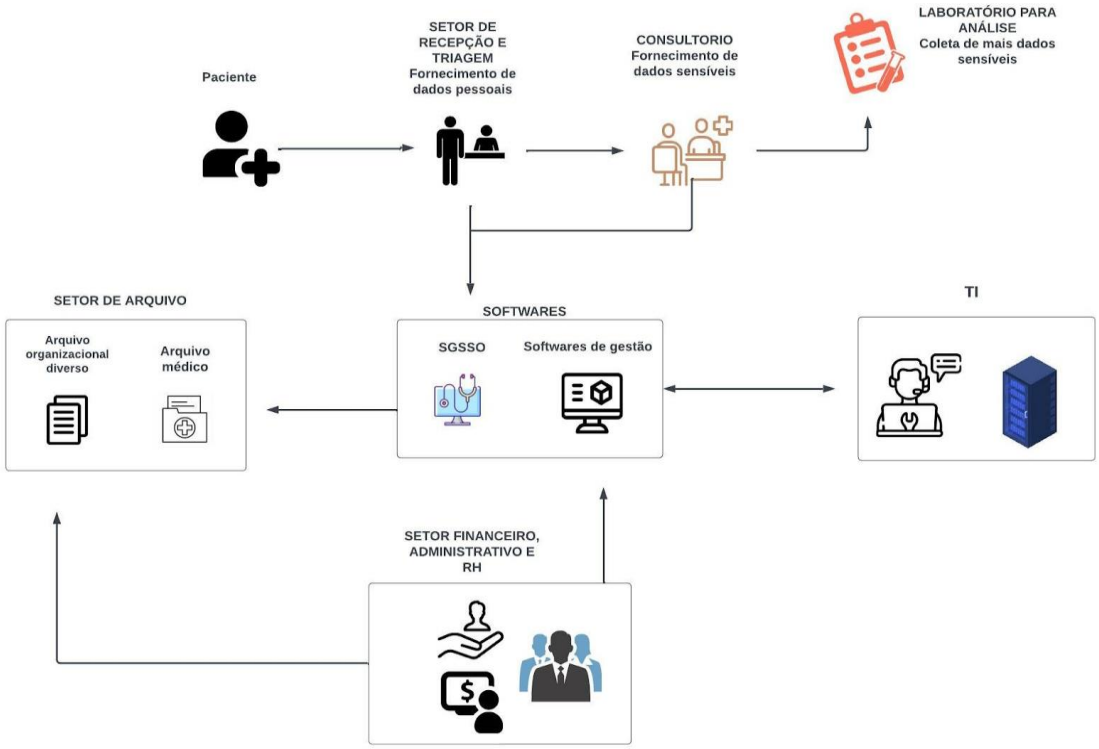


Fonte: A autora (2022)

5.1.1 Fluxos e ciclo de vida dos dados sensíveis - Clínica Med&Clinic

Desde a entrada e atendimento do usuário, até a finalização dos processos, há tratamento de dados na clínica. Esse trânsito de etapas é definido como ciclo dos dados e entender essa movimentação é importante para analisar possíveis vulnerabilidades presentes no cenário. O ciclo apresentado a seguir tem como base o ciclo de vida dos dados no setor de saúde.[13]

Figura 10 - Ciclo de dados - clínica Med&Clinic



Fonte: A autora (2022)

- **Processo da recepção:** Ao entrar na clínica o paciente fornece primeiramente os dados pessoais ao setor da recepção. Após o fornecimento dos dados, o paciente aguarda o chamado para recebimento de exames já expedidos (setor de arquivo médico) ou para realizar consultas.
- **Triagem e consulta médica:** Após a recepção, o paciente segue para a triagem. A triagem caracteriza-se pelo "filtro" antes da consulta, sendo a parte que envolve o fornecimento inicial de dados sensíveis através da execução da *anamnese.* Esse processo

[13] CONFEDERAÇÃO NACIONAL DA SAÚDE. **CÓDIGO DE BOAS PRÁTICAS:** Proteção de dados para prestadores privados em saúde. Disponível em: http://cnsaude.org .br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em 19 de fevereiro de 2022.

pode ser feito tanto em fichas físicas ou em sistemas de software de saúde, com cópias destinadas ao setor de arquivo.

Após a triagem, o paciente segue para o consultório, onde fornece mais informações sensíveis para o médico. Esse fornecimento acaba sendo necessário para a construção e registro do prontuário.

- **Setor de arquivo:** A sala do arquivo é constituída pelo conjunto de documentos relacionados a atendimentos prestados aos pacientes, além de outros documentos importantes à clínica. Cópias de documentos médicos, fichas, prontuários e outros documentos organizacionais seguem para esse setor.
- **Setor de TI:** relacionado às prestações de serviços de tecnologia da informação. Além do operacional e suporte técnico, a sala possui os servidores que também armazenam informações médicas.
- **Financeiro, RH e administrativo:** Apesar de serem setores que não lidam constantemente com dados sensíveis, também são setores que englobam dados de caráter sigilosos. Boa parte dos processos envolvem documentação de caráter físico, embora haja a utilização de softwares de gestão.

5.1.2 Vulnerabilidades no fluxo de dados - Clínica Med&Clinic

Ao analisar o cenário na empresa Med&Clinic e tomar como base o fluxo de dados, são observadas as possíveis vulnerabilidades:

1. “Ao entrar na clínica, o paciente fornece dados pessoais para serem anexados a um cadastro. Um software de saúde e gestão ocupacional é utilizado para armazenamento e localização de informações, onde o mesmo emite fichas físicas e digitais que serão direcionadas ao setor de arquivo médico, bem como armazenadas no banco de dados”.

Não há um termo de compromisso para o fornecimento de dados ao entrar na recepção, ou seja, o paciente não tem conhecimento de como serão tratados os dados. O acesso ao sistema de gestão (*login*) é um ponto importante para ser visto, bem como suas permissões para visualização dos dados (conforme A.9.4.2 - Procedimentos seguros de entrada no sistema – ISO 27001).

2. “Após a triagem, o paciente é chamado ao consultório, onde o médico coleta dados sensíveis para prosseguir com o prontuário e mais a frente com o diagnóstico. Essas

informações podem ser alergias a medicamentos, atividades de rotina, históricos de doenças ou fatores de risco em geral".

Fichas de diagnóstico, prontuário e receituário, são armazenadas, bem como impressas. Toda a análise desse armazenamento é importante, visto que a quantidade de dados sensíveis aumentou. O acesso e restrição no SGSSO (conforme Anexo A – seção 9.4.1 – ISO 27001) deve ser averiguado, já que o acesso médico deve ser totalmente diferente de um outro colaborador (como a recepção, por exemplo).

3. "Para obter maior embasamento no diagnóstico, o médico também pode exigir exames laboratoriais adicionais. Após consulta, a cópia dos dados e procedimentos seguem para armazenamento no arquivo médico".

A exigência de exames adicionais, como os de laboratórios, também inclui mais dados sensíveis (e pode incluir uma tratativa de dados realizados por terceiros). Quanto ao armazenamento, para o arquivo digital, é importante verificar a acessibilidade, a proteção e a permissão de acesso aos dados. Os mesmos critérios serão definidos para o arquivo físico, com o adicional do acesso às salas, manutenção (visto que o mesmo poderá sofrer avarias devido ao tempo, umidade ou incêndio) e ao manuseio (Conforme Anexo A – seção 11.1 - Áreas seguras – ISO 27001). Qual será o critério de controle para o acesso?

4. "O TI possui os servidores de armazenamento e operações dos sistemas SGSSO. O RH e o financeiro não trabalham diretamente com o ciclo de dados sensíveis".

O TI é a central onde ficam armazenados os sistemas de gestão, bem como os *backups* de informações críticas. Verificar o acesso à sala, estado físico e lógico dos servidores, atualizações, utilização de *firewall*, bem como a rotina dos backups faz parte do conjunto de critérios importantes para proteção dos dados.

Mesmo que os setores de RH e financeiro não lidem diretamente com documentação médica, as documentações dos setores são importantes, devendo ser tratadas de forma cuidadosa. A aplicação da política de mesas limpas (conjunto de práticas de segurança da informação que evitam a exposição de informações) podem ajudar a determinar como estão sendo tratados os documentos do setor (conforme Anexo A - seção 11.2.9 – ISO 27001).

5.2 Análise e avaliação de risco - Clínica Med&Clinic

A análise de risco é necessária para a tomada de decisões relacionadas à proteção dos dados na clínica Med&Clinic. Para a sua construção, após o alinhamento de objetivos

relacionados com o TI e a administração, é necessário a identificação dos ativos, das vulnerabilidades, dos riscos da organização e por último o controle ou aceitação do risco.

5.2.1 Identificação e classificação dos ativos

Ativo é tudo que tem como referência os bens da organização, sendo adquiridos pelo capital próprio ou por terceiros, conforme Hintzbergen (2018). No contexto da segurança da informação, o ativo é um elemento informacional, como documentos, base de dados, programas, ou equipamentos como servidores, devendo ser protegido conforme execução do ciclo CIA.

Na Med&Clinic, os ativos relacionados à segurança da informação podem ser listados de acordo a tabela a seguir:

Tabela 7 - Análise de ativos - Clínica Med&Clinic

Ativo	Tipo de ativo	Setor localizado
Fichas de cadastro	Ativo físico ou digital	Recepção e triagem
Modelos de relatorios	Ativo físico ou digital	Recepção, triagem, financeiro, administrativo,RH
Relatório médico	Ativo físico ou digital	Consultorio médico/ arquivo médico
Receituário	ativo físico ou digital	Consultorio médico/ arquivo médico
Servidores	Ativo físico	TI
Anotações /lembretes e recados simples	Ativo em boa parte das vezes físico	Setores diversos
Contratos organizacionais	Ativo físico ou digital	Financeiro, Administrativo
Softwares de gestão organizacional e SGSSO	Ativo digital	Financeiro,Administrativo e setores fora do contexto médico utilizam os softwares de gestão
curriculos, fichas de colaboradores	Ativo físico ou digital	RH
Firewall/ antivirus/ softwares de proteção	Ativo digital	TI

Fonte: A autora (2022).

Ao analisar a tabela, será feita a classificação dos ativos, conforme especificação da ISO 27001 (Anexo 8.2 - Classificação da informação). Essa forma de classificação irá facilitar a escolha de métodos de proteção mais adequados, de acordo com a criticidade:

Tabela 8 - Classificação de ativos - Clínica Med&Clinic

Ativo	Tipo de ativo	Setor localizado	Classificação
Fichas de cadastro	Ativo físico ou digital	Recepção e triagem	**Restrito**
Modelos de relatorios	Ativo físico ou digital	Recepção, triagem, financeiro, administrativo,RH	**Interno**
Relatório médico	Ativo físico ou digital	Consultorio médico/ arquivo médico	**Confidencial**
Receituário	ativo físico ou digital	Consultorio médico/ arquivo médico	**Confidencial**
Servidores	Ativo físico	TI	**Confidencial**
Anotações /lembretes e recados simples	Ativo em boa parte das vezes físico	Setores diversos	**Interno**
Contratos organizacionais	Ativo físico ou digital	Financeiro, Administrativo	**Restrito**
Softwares de gestão organizacional e SGSSO	Ativo digital	Financeiro,Administrativo e setores fora do contexto médico utilizam os softwares de gestão	**Interno/ restrito (de acordo ao acesso dentro do software)**
curriculos, fichas de colaboradores	Ativo físico ou digital	RH	**Restrito**
Firewall/ antivirus/ softwares de proteção	Ativo digital	TI	**Confidencial**

Fonte: A autora (2022).

- **Confidencial:** Ativo que possui grande risco caso sofra um dano como exposição ou avaria, devendo estar num nível alto de proteção.
- **Restrito:** Ativo para uso em setores específicos, com nível médio de proteção.
- **Interno:** Ativo de uso geral da organização, com nível baixo de proteção.
- **Público:** ativo para uso geral, sem grandes impactos de proteção, devendo apenas ser protegido em critérios de disponibilização e integralização.

5.2.2 Identificação das vulnerabilidades

Tomando como base a classificação dos ativos são observadas as possíveis vulnerabilidades:

- **Fichas de cadastro, relatórios, anotações e fichas de colaboradores (classificação restrita a interna):** A vulnerabilidade de fichas e cadastros está relacionada à exposição desnecessária através de ações como documentos deixados em mesas de trabalho, balcões, quadros ou acessos a computadores sem bloqueio e outras mídias eletrônicas. Marcondes (2021) também reforça que impressões desprotegidas assim como a destruição incorreta de documentos também são vulnerabilidades que geram o comprometimento da informação.

- **Receituários e outros documentos sensíveis:** Às mesmas vulnerabilidades observadas anteriormente podem ser atribuídas a documentação médica, com o agravante que tais documentos são sensíveis, o que aumenta o impacto em casos de possíveis ameaças.
- **Salas e controles físicos:** Salas de servidores e sistemas centralizados sem controle de entrada possuem vulnerabilidades de acesso. Além disso, a falta de dispositivos e métodos relacionados à manutenção e proteção de ativos, como extintores, *sprinklers*, e desumidificadores são falhas de preservação dos ativos.
- **SGSSO e outros sistemas de gestão:** Senhas fáceis, falhas de autorização e criptografia, falhas de disponibilidade, falhas de autenticação e backup são vulnerabilidades em *softwares.*
- **Servidores:** Além do acesso facilitado a sala, falhas de backups, conservação (proteção contra incêndios, falhas elétricas e derivados) e operação (portas abertas no firewall, falta de atualizações, senhas frágeis) caracterizam-se como vulnerabilidades.

Tabela 9 - Classificação de vulnerabilidades: Clínica Med&Clinic

Ativo	Tipo de ativo	Setor localizado	Classificação	Vulnerabilidades apresentadas
Anotações /lembretes e recados simples Modelos de relatorios	Ativo físico ou digital	Setores diversos	Interno	Documentação exposta em mesas, balcões, quadros ou impressoras. Eliminação incorreta de documentos. Visualização de fichas em computadores com sessões abertas. Setores e salas com fácil acessibilidade.
Fichas de cadastro Contratos organizacionais curriculos, fichas de colaboradores	Ativo físico ou digital	Recepção, triagem, financeiro, administrativo,RH	Restrito	
Relatório médico Receituário	Ativo físico ou digital	Consultorio médico arquivo médico	Confidencial	
Servidores e seus tipos: Firewall, antivirus, arquivos, web	Ativo físico	TI	Confidencial	Acesso facilitado a sala Falhas de backup Falhas de manutenção (proteção contra incêndios, falhas elétricas e derivados) Falhas de operação (Portas abertas no firewall, falhas em atualizações e senhas frágeis)
Salas e controles físicos:	Ativo físico	Setores diversos	Interno Restrito confidencial	Falta de dispositivos e métodos relacionados à manutenção e proteção de ativos: extintores, sprinkler e desumidificadores Acesso facilitado as salas
SGSSO e outros softwares de gestão	Ativo digital	TI (servidores)	Interno ou restrito (de acordo ao acesso dentro do software)	Senhas fáceis, Falhas de autorização e criptografia, falhas de disponibilidade e backup Falha de autenticação

Fonte: A autora (2022)

5.2.3 Avaliação dos riscos nos processos

Os riscos têm a propriedade de corromper os ativos através das ameaças e vulnerabilidades, ferindo os padrões CIA. Após a abordagem das vulnerabilidades da clínica Med&Clinic, parte-se para a descrição dos possíveis riscos:

Tabela 10 - Avaliação dos riscos - Clínica Med&Clinic

Ativo	Tipo de ativo	Setor localizado	Classificação	Vulnerabilidades apresentadas	Potenciais riscos
Anotações /lembretes e recados simples Modelos de relatorios	Ativo físico ou digital	Setores diversos	Interno	Documentação exposta em mesas, balcões, quadros ou impressoras. Eliminação incorreta de documentos. Visualização de fichas em computadores com sessões abertas. Setores e salas com fácil acessibilidade.	Roubo de dados Vazamento de dados Avaria permanente aos dados e outros ativos
Fichas de cadastro Contratos organizacionais curriculos, fichas de colaboradores	Ativo físico ou digital	Recepção, triagem, financeiro, administrativo,RH	Restrito		
Relatório médico Receituário	Ativo físico ou digital	Consultorio médico arquivo médico	Confidencial		
Servidores e seus tipos: Firewall, antivirus, arquivos, web	Ativo físico	TI	Confidencial	Acesso facilitado a sala Falhas de backup Falhas de manutenção (proteção contra incêndios, falhas elétricas e derivados) Falhas de operação (Portas abertas no firewall, falhas em atualizações e senhas frágeis)	Ataques de ransomware ataques de negação de serviço (DDoS) Perda de dados Interrupção de serviços
Salas e controles físicos:	Ativo físico	Setores diversos	Interno Restrito confidencial	Falta de dispositivos e métodos relacionados à manutenção e proteção de ativos: extintores, sprinkler e desumidificadores Acesso facilitado as salas	Avaria permanente aos ativos
SGSSO e outros softwares de gestão	Ativo digital	TI (servidores)	Interno ou restrito (de acordo ao acesso dentro do software)	Senhas fáceis, Falhas de autorização e criptografia, falhas de disponibilidade e backup Falha de autenticação	Roubo de dados Vazamento de dados

Fonte: A autora (2022)

Boa parte dos riscos associados estão relacionados ao vazamento de informações e dados, bem como à inutilização dos ativos, ocasionado pela falta de manutenção e cuidado dos acessos físicos.

5.2.4 Controle ou aceitação do risco

Após a identificação dos riscos será decidido como a organização irá lidar com eles. Há formas que poderão ser escolhidas, a depender se a organização decidir aceitar ou não os riscos presentes:

- **Controle de risco:** A organização adotará medidas para reduzir a incidência dos riscos, seja mitigando ou eliminando as ameaças. Para esse controle deve ser levado em conta a aplicação de controles adequados, a transferência do risco para seguradoras e tentar evitar ações que possam causar a ocorrência de novos riscos.
- **Aceitação:** Nesse caso, o risco será aceito quando a organização percebeu que o mesmo é baixo, ou não possui um tratamento rentável. É interessante entender que a aceitação deve ocorrer somente se esse processo estiver de acordo com a política e os requisitos de aceitação da organização.

Conforme a tabela 10, e seguindo as seções do anexo A da ISO 27001 (Referência aos controles e objetivos de controles) são sugeridas as seguintes orientações para controle do risco:

- **Documentos confidenciais e restritos expostos (Setores gerais, conforme anexo A - seção 11.2 - Equipamentos):** É necessário adotar políticas onde protejam os

documentos e informações (política da mesa limpa). Na clínica Med&Clinic, os documentos físicos deverão ser guardados após horário de trabalho (gavetas e salas trancadas), não devendo ser exibidos e colados em painéis ou murais. A visualização dos documentos sensíveis (fichas médicas, prontuários, etc.) e confidenciais precisam de restrição, cabendo apenas aos colaboradores permitidos a acessibilidade.

- **Eliminação incorreta de documentos (Setores gerais, conforme anexo A - seção 8.3 - Tratamento de mídias):** Documentos deverão ser destruídos, de forma que não possam ser recuperados. Os papéis deverão ser fragmentados e eliminados em lixo separado. Como forma prática, deverá ser utilizado na clínica Med&Clinic um fragmentador de papéis. Mídias eletrônicas, HDs e outros dispositivos de armazenamento devem passar por processos de exposição magnética/destruição manual e fragmentação. O reaproveitamento do dispositivo poderá ser feito, contato que o mesmo tenha os dados apagados/sobrescritos.

- **Segurança nos contratos (RH e setores administrativos, conforme anexo A - seção 7- Segurança em recursos humanos):** Na clínica Med&Clinic os funcionários precisarão ter acesso às políticas de segurança da informação, assim como treinamentos e medidas de conscientização para cumprimento das exigências de tratamento dos dados. Além da política, devem ser aplicadas as medidas disciplinares (para caso de descumprimento na proteção dos dados) e medidas externas (para colaboradores que forem desligados da empresa).

- **Acessos de seções online (Setores gerais, conforme anexo A - seção 9.4 - Controle de acesso ao sistema e à aplicação):** Será verificada as seções dos colaboradores da Med&Clinic, onde será orientado que as mesmas não poderão ser deixadas “abertas”. As telas que exibem informações (principalmente sensíveis) devem ser posicionadas de forma estratégica, evitando visualização em campo amplo. Todas as seções de colaboradores precisam ter senhas fortes (a especificar, conforme orientação do setor de TI).

- **Acesso ao sistema SGSSO e outros softwares (Setores gerais, conforme anexo A - seção 9.4 - Controle de acesso ao sistema e à aplicação):** O SGSSO utilizado na clínica Med&Clinic precisa ter camadas de restrição. Um acesso médico deve ser diferente de um atendente. Softwares de gestão administrativa também devem ter critérios de acesso. As senhas precisam ser fortes, possuindo uma sequência qualitativa.

- **Segurança da rede (Setor de TI, conforme anexo A – seção 13.1 - Gerenciamento da segurança em redes):** As portas do firewall deverão ser verificadas, conforme análise do(s) especialista(s) em TI. Serão verificadas irregularidades referentes às atualizações, bem como os grupos de acesso e permissões.
- **Backups (Setor de TI, conforme anexo A - Seção 12.3 - Cópias de segurança):** O setor de TI da Med&Clinic deverá estabelecer uma escala, onde realizará operações de cópias dos dados. As mesmas deverão ser testadas regularmente, bem como armazenadas de forma confidencial e segura.
- **Acesso às salas e proteção física (Setores gerais, conforme anexo A - seção 11 - Segurança física e do ambiente):** Todas as áreas da clínica Med&Clinic que possuam ativos de caráter restrito e confidencial precisam ter métodos de controle para entrada (biometria, chaves, fechaduras digitais). As chaves, que deverão ficar em claviculário, precisam ter controle absoluto. Além da proteção em acesso, proteções externas e naturais deverão ser implantadas, como extintores, detectores de incêndio, proteções contra umidade e raios.

A visualização dos controles sugeridos de risco para a clínica Med&Clinic será melhor exemplificada no Apêndice B.

6 MODELO PROPOSTO

6.1 Modelo proposto de controle de risco hierárquico - Clínica Med&Clinic

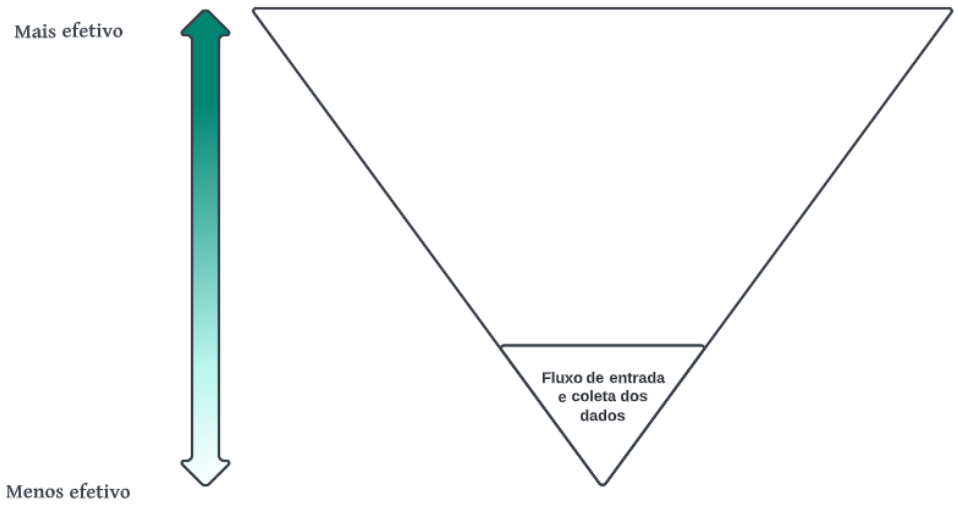
Conforme descrito no capítulo dois, a escolha de um modelo hierárquico de controle de risco ocupacional modificado para a segurança de dados sensíveis seria efetivo para auxiliar na tomada de melhores abordagens para a proteção dos dados. Tomando como base a análise de vulnerabilidades e possíveis riscos na clínica Med&clinic descritos no capitulo cinco, bem como a estruturação do modelo de controle de risco HOC - ISO 45001(Capitulo 8: Operação) parte-se para a construção e apresentação do modelo de proteção hierárquico de dados sensíveis.

6.1.1 Fluxo de entrada e coleta dos dados sensíveis

Para a construção da primeira base da hierarquia de controle de risco foi levado em consideração dois pontos importantes: os processos de coleta e a entrada dos dados sensíveis. Entende-se que o primeiro cuidado está relacionado a como a coleta dos dados sensíveis acontece e qual a justificativa para tal ação.

Deve ser esclarecido ao usuário a autorização e a finalidade da coleta dos dados sensíveis. Essa primeira restrição no processo de entrada dos dados é uma ação que visa reduzir o impacto de futuras sanções jurídicas e administrativas para a organização.

Figura 11 - Hierarquia de controle de risco - Fluxo de entrada e coleta dos dados



Fonte: A autora (2022)

A primeira tomada hierárquica de decisão protege os dados sensíveis porque esclarece como os mesmos serão tratados e o porquê serão coletados. Todavia, a efetividade do

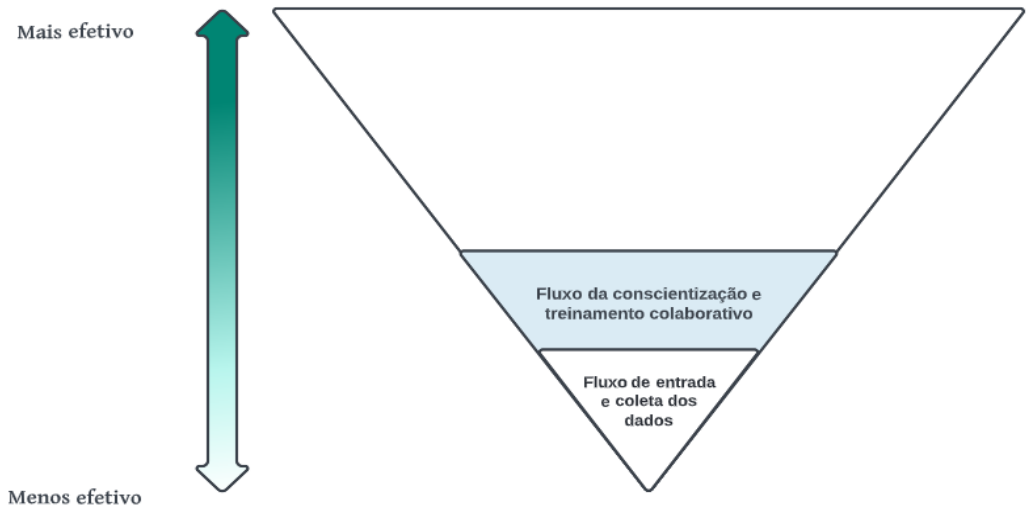
procedimento é mínima, visto que somente o consentimento não é suficiente para a proteção dos dados sensíveis.

Como política para o controle de risco da primeira camada hierárquica, tem-se o termo de compromisso, onde deverá ter especificada a finalidade da coleta e a descrição do compartilhamento dos dados (Ver Apêndice C - Modelo de termo de compromisso para tratamento dos dados).

6.1.2 Fluxo de conscientização e treinamento colaborativo

A segunda etapa no controle de risco hierárquico envolve os colaboradores e suas responsabilidades na organização. Todas as pessoas dentro da organização precisam conhecer as políticas de segurança da informação, assim como o código de conduta que deverá ser aplicado no caso de não cumprimento das medidas. Quando um funcionário é efetivado, a organização necessita prover treinamentos e conscientização acerca dos procedimentos de segurança da informação escolhidos (Conforme ISO 27001 – anexo A - seção 7.2.2 - Conscientização, educação e treinamento em segurança da informação).

Figura 12 - Hierarquia de controle de risco - Fluxo de conscientização e treinamento colaborativo



Fonte: A autora (2022)

Conscientizar o colaborador envolve muito mais do que dizer quais normas devem ser seguidas, mas sim tentar demonstrar a importância de proteger os dados, passos estes que podem ser utilizados não somente no âmbito da empresa, mas fora desta. Como segunda camada do controle de risco hierárquico, o treinamento colaborativo possui efetividade acima dos termos de consentimento e compromisso porque além de informar sobre diretrizes de

segurança, possui o fator de incentivar os colaboradores e outros auxiliares dos serviços médicos a protegerem os dados sensíveis, bem como a se preocuparem com possíveis impactos acerca da exposição desnecessária.

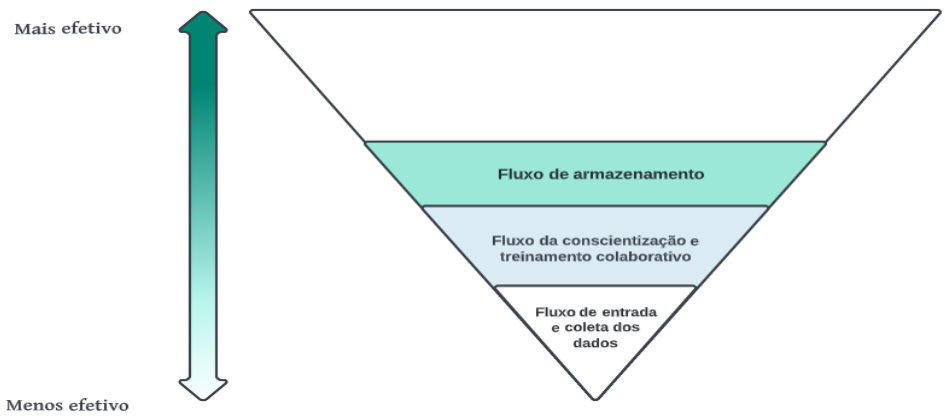
Essa camada possui efetividade mínima / média porque independente da força de contribuição, só o conhecimento dos colaboradores acerca das responsabilidades de segurança da informação e dados não é suficiente para a proteção dos dados sensíveis acerca da engenharia social e seus impactos. Hintzbergen (2018), afirma que intencionalmente as pessoas podem causar danos aos sistemas de informação e por mais que pensamos que esses intrusos venham de maneira externa com o interesse de invadir a empresa, ataques podem ser feitos por funcionários descontentes e ou vingativos.

Como política para o controle de risco da segunda camada hierárquica, tem-se o treinamento para os colaboradores (palestras, cursos, descrição de diretrizes, documentações e informativos disponibilizados para os setores e outros treinamentos).

6.1.3 Fluxo de armazenamento dos dados sensíveis

Armazenar nada mais é do que reter as informações e dados, utilizando algum mecanismo digital ou físico, com o intuito de se obter o acesso conforme necessário. Foi visto anteriormente que para o armazenamento podem ser utilizadas mídias como CDs e HDs, assim como arquivos físicos e digitais. A escolha do fluxo de armazenamento como terceira camada no controle de risco dos dados sensíveis ocorreu pelo seguinte ponto: Após a coleta de dados, a efetividade aumenta quando é escolhida uma forma de armazenamento para o dado sensível, o que modifica a acessibilidade e proteção.

Figura 13 - Hierarquia de risco - fluxo de armazenamento



Fonte: A autora (2022)

A efetividade no armazenamento dos dados sensíveis se dá pela proteção e aumento do gerenciamento, através da utilização de mecanismos escolhidos pela organização (banco de dados, arquivos, etc). As operações de dados são melhores otimizadas quando o armazenamento é efetivo, visto que o acesso se torna mais ágil. Entende-se que uma forma de armazenamento simples para o dado sensível (como uma folha de papel) possui grau de efetividade menor do que um HD, devido a facilidade de leitura. Essa efetividade, entretanto, pode ser modificada se a forma de armazenamento possuir um grau elevado de acesso. A folha de papel com dado sensível pode estar localizada em um arquivo com difícil acessibilidade, e o HD, que não possui criptografia, pode ser facilmente conectado em um dispositivo e lido).

O armazenamento ajuda a categorizar e otimizar a busca de possíveis informações e dados, possuindo efetividade média. Sua fraqueza está em como o acesso é realizado, ou seja, como e quem poderá acessar os dados sensíveis.

Como política para controle de risco da terceira camada de controle hierárquica, tem-se os métodos de armazenamento e organização dos dados sensíveis (dispositivos digitais, dispositivos físicos, a depender da escolha da organização), o que garante a integridade e a maior acessibilidade de dados.

6.1.4 Fluxo de compartilhamento dos dados sensíveis

A primeira camada da hierarquia possuía como controle de risco, o termo de consentimento. Solicitar o consentimento para o usuário minimiza possíveis riscos aos dados sensíveis. Entretanto, o consentimento não deve ser somente relacionado às operações de coleta, mas sim do compartilhamento.

As trocas dos dados de caráter sensível são cruciais para cenários médicos, tanto como forma de prestação de serviços, como para outras funções organizacionais. Leis de proteção de dados (como a LGPD[14]) não proíbem o compartilhamento de dados sensíveis, visto que esse compartilhamento muitas vezes é necessário para processos operacionais nas áreas de saúde. Porém o compartilhamento deve ser restrito o máximo possível, priorizando o consentimento.

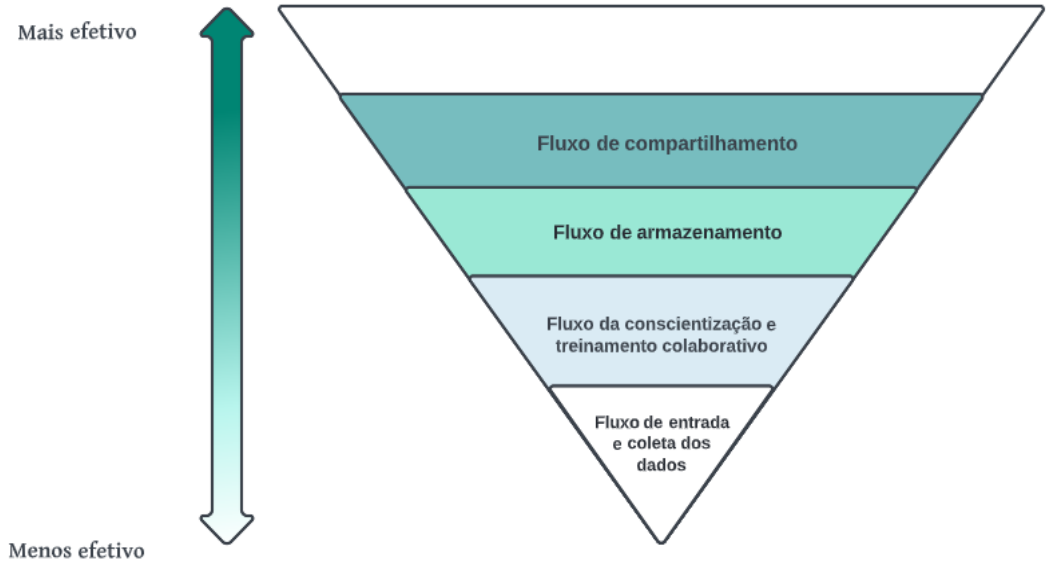
A utilização de plataformas de comunicação (como mensageiros eletrônicos) também não é vetada para o compartilhamento de dados sensíveis. É entendido, conforme código de

[14] BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD),** nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709. htm. Acesso em 16 de setembro de 2021.

conduta médica (Parecer nº 14/2017[15]) que a utilização de recursos tecnológicos beneficia o profissional de saúde na obtenção do diagnóstico, porém para a utilização de tais tecnologias, a exibição e identificação de pacientes em grupos e outros assuntos médicos é expressamente proibida.

Como construção da quarta camada tem-se a camada do compartilhamento, devendo esse processo ser o mais restrito possível, devido ao grau de impacto dos dados sensíveis em caso de eventos de ameaça.

Figura 14 - Hierarquia de risco - fluxo de compartilhamento



Fonte: A autora (2022)

As políticas de controles de risco que podem ser aplicadas para a quarta camada são:

- O consentimento dado pelo usuário para o caso de compartilhamento, período de armazenamento e eliminação dos dados sensíveis (também presente na primeira camada).
- Para o compartilhamento entre profissionais de saúde, grupos em mensageiros instantâneos devem ser exclusivos a profissionais registrados em conselhos médicos.
- O dado compartilhado não pode identificar o paciente, assim como não poderá ser utilizado para fins de anúncios e outros benefícios médicos. Participantes de grupos,

[15] CONSELHO REGIONAL DE MEDICINA – CRM. PROCESSO - CONSULTA CFM nº50/2016–PARECER CFM nº14/2017. **Uso do WhatsApp em ambiente hospitalar.** Disponível em: https://sistemas.cfm.org.br/normas/visualizar/pareceres/BR/2017/14. Acesso em: 05 de julho de 2022.

comitês e outras organizações, digitais ou não, são os responsáveis pelas informações e tratamento aos dados sensíveis, devendo manter a ética e sigilo médico.

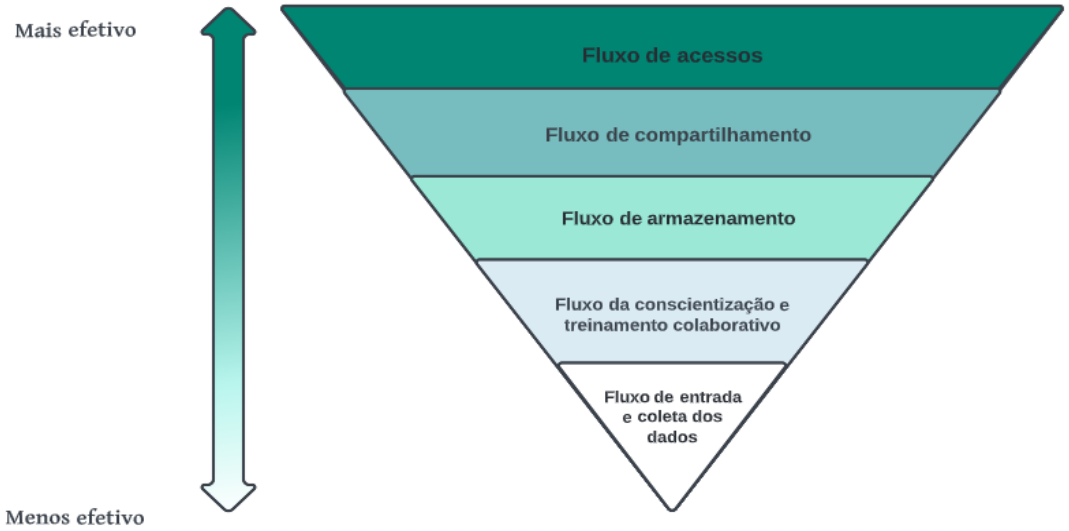
- O compartilhamento de dados sensíveis por terceiros, como entre a instituição de saúde e laboratórios, só deve acontecer em casos estritamente necessários, prezando também o consentimento.

6.1.5 Fluxo de acessibilidade aos dados sensíveis

Na terceira hierarquia foi visto que o armazenamento melhora a forma como os dados e informações sensíveis são administradas. Vendo pelo ponto da segurança da informação, só o armazenamento não é suficiente já que a forma de acesso pode ocasionar danos e perdas aos dados sensíveis. Os dados não precisam apenas ser bem armazenados, mas também precisam possuir medidas para bloquear acessos não autorizados.

Para reduzir riscos relacionados ao acesso não autorizado, é necessário a adoção de políticas que evitem o manuseio sem autorização dos dados sensíveis. Políticas de controle de acesso possuem efetividade alta porque atuam como "fiscalizadores" entre o processo de obtenção dos dados, limitando possíveis tratamentos não concedidos.

Figura 15 - Hierarquia de risco - fluxo de acessos



Fonte: A autora (2022).

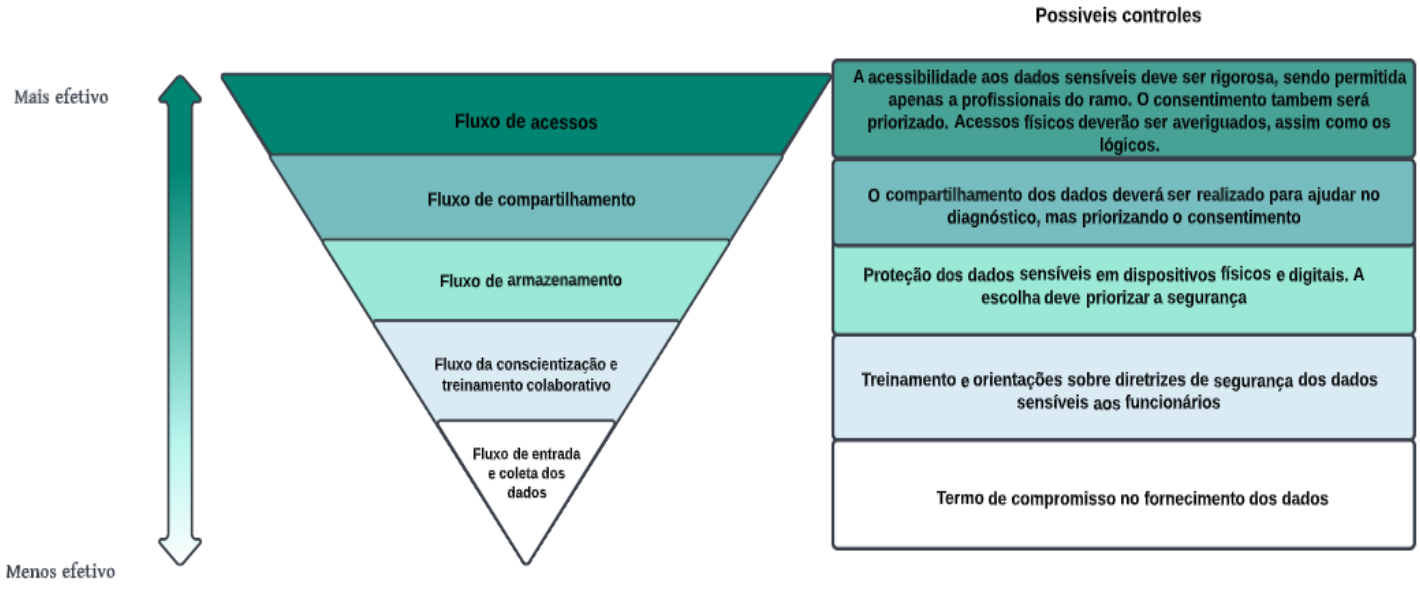
Quanto ao fluxo de acesso, existem diversas políticas para controle de risco, divididas em acessibilidade virtual e física, onde:

- **Acessibilidade física:** Criar o perímetro de segurança (conforme ISO 27001 – anexo A - seção 11.1.1- perímetro de segurança física), protegendo as áreas onde estão localizados os dados sensíveis, assim como a entrada, que deve possuir mecanismos de proteção que evitem o acesso de colaboradores sem permissão.
- **Acessibilidade lógica:** Impedir acessos digitais facilitados, utilizando para isso, mecanismos que inibam os acessos: *logins*, verificações em duas etapas, criptografia, etc. Revisar sempre que possível as permissões, assim como ajustar ou cancelar as permissões concedidas caso necessário.

6.2 Aplicabilidade do modelo hierárquico de controle de risco - Clínica Med&Clinic

Por fim, tomando como exemplo o modelo hierárquico construído e analisando com o cenário da clínica Med&Clinic tem-se as seguintes ações de controle:

Figura 16 - Possíveis controles e aplicabilidades do controle de risco hierárquico



Fonte: A autora (2022)

7 CONCLUSÃO

O presente trabalho teve como objetivo a apresentação e construção de um modelo hierárquico para controle de risco de dados sensíveis, baseado na estrutura de segurança ocupacional (ISO 45001). Trazer uma estrutura de mitigação de riscos ocupacional para o ambiente de proteção dos dados foi visto como uma proposta interessante para auxiliar no tratamento dos dados, através da premissa de seguir passos por uma hierarquia organizacional. A iniciativa de aplicar esse modelo para dados sensíveis teve como base a grande quantidade de tratamento desses dados em cenários médicos. Nesses locais são necessárias análises de fluxo e ciclos para evitar diversos riscos para os titulares em casos de avarias ou vazamentos desses dados.

Para a criação do modelo hierárquico foram definidos três objetivos específicos. Primeiramente, foram descritas possíveis vulnerabilidades que estariam relacionadas ao tratamento dos dados sensíveis. A partir daí foi descrito o risco, bem como a análise de risco e a importância de determinar ameaças e os possíveis passos que seriam seguidos para combatê-las. Na apresentação dos dados sensíveis, foi evidenciado que devido às características específicas o impacto seria mais grave caso os mesmos sofressem ataques, e, portanto, a proteção deveria ser mais rigorosa.

Foram apresentadas soluções paliativas que eram escolhidas para mitigação do risco, e como essas técnicas eram insuficientes. A partir daí foi mostrado como um modelo hierárquico de controle poderia ser utilizado para facilitar a tomada de decisões, de uma maneira mais intuitiva e organizada.

Inicialmente, apesar do interesse central que a pesquisa pudesse ser aplicada em um ambiente real de grande porte, a criação de uma clínica fictícia foi escolhida para ilustrar de forma mais simples como dados sensíveis eram tratados, sem envolver grandes fluxos, como o de um ambiente hospitalar.

Devido a ser um ciclo de dados com organograma pequeno, a criação do modelo não foi extremamente trabalhosa. Cada camada pôde ser bem aplicada aos processos da clínica em questão, aliando a organização dos processos de controle e a etapa dos passos que seriam tomados para resguardar os dados. Entretanto, uma situação que foi notada foi que o controle construído também poderia ser aplicado aos dados não sensíveis, visto que o mesmo se adequa bem a outras tomadas de decisão que envolvam operações de controle e proteção a dados.

Uma dificuldade sentida na construção da hierarquia foi o alinhamento da mesma com diversas regulamentações de proteção dos dados, assim como a tentativa de alinhar as

camadas com todos os cenários dentro da clínica fictícia. A construção de uma análise de risco foi um desafio, a se compreender pelos diversos setores e possíveis fluxos de dados que poderiam ser imaginados. Em contrapartida, a utilização das ISOs ajudou a direcionar o trabalho, principalmente na utilização dos anexos.

Devido a apresentação e organização intuitiva no controle e tratamento dos dados, em pesquisas futuras a hierarquia de controle pode ser implementada para outros cenários que não tivessem especificamente dados sensíveis, mas que possuíssem grande fluxo de dados que necessitassem das avaliações de segurança no tratamento.

REFERÊNCIAS

AVAST ACADEMY. **Ransomware Petya: Como funciona e como se proteger.** Disponível em: www.avast.com/pt-br/c-petya. Acesso em 13 de outubro de 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001: Sistemas de gestão de segurança da informação: requisitos.** Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005: Técnicas de segurança: gestão de riscos de segurança da informação**. Rio de Janeiro, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 45001: Sistemas de gestão de saúde e segurança ocupacional: requisitos**. Rio de Janeiro, 2018.

BISSO, Rodrigo, et al. **Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados (versão estendida).** Disponível em: https://revistas. setrem.com.br/index.php/reabtic/article/view/378/174. Acesso em 27 de setembro de 2021.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD),** nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709. htm. Acesso em 16 de setembro de 2021.

CAMPOS, Claudinei José Gomes; FONTANELLA, Bruno José Barcellos; TURATO, Egberto Ribeiro. **COLETA DE DADOS NA PESQUISA CLÍNICO-QUALITATIVA:** uso de entrevistas não dirigidas de questões abertas por profissionais da saúde. Disponível em: https://www.scielo.br/j/rlae/a/KhvFsGT6xf5yxKXTqQ5PkRN/?format=pdf&lang=pt. Acesso em 06 de fevereiro de 2022.

COMISSÃO EUROPEIA. **Que dados pessoais são considerados sensíveis?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_pt. Acesso em 28 de setembro de 2021.

CONECTA JÁ - PROTESTE. **LGPD: O que são dados pessoais sensíveis.** Disponível em: https://conectaja.proteste.org.br/lgpd-o-que-sao-dados-pessoais-sensiveis/. Acesso em 16 de setembro de 2021.

CONFEDERAÇÃO NACIONAL DA SAÚDE. **CÓDIGO DE BOAS PRÁTICAS:** Proteção de dados para prestadores privados em saúde. Disponível em: http://cnsaude.org .br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em 19 de fevereiro de 2022.

CONSELHO REGIONAL DE MEDICINA – CRM. PROCESSO - CONSULTA CFM nº50/2016–PARECER CFM nº14/2017. **Uso do WhatsApp em ambiente hospitalar.** Disponível em: https://sistemas.cfm.org.br/normas/visualizar/pareceres/BR/2017/14. Acesso em: 05 de julho de 2022.

CRYPTOID. **Ransomware: maioria dos brasileiros paga resgate, mas menos de um terço tem dados devolvidos.** Disponível em: https://cryptoid.com.br/identidade-digital-destaques/ransomware-maioria-dos-brasileiros-paga-resgate-mas-menos-de-um-terco-tem-dados-devolvidos/. Acesso em 02 de outubro de 2021.

DELPHOS. **5 Formas de proteger dados sensíveis.** Disponível em: https://www.delphos.com.br/5-formas-de-proteger-dados-pessoais/. Acesso em 16 de setembro de 2021**.**

DURBANO, Vinicius. **Gestão de riscos: qual a importância dela na área de TI.** Disponível em: https://blog.ecoit.com.br/gestao-de-riscos/. Acesso em 07 de outubro de 2021.

ELIAS, Diego. **Dados VS informação:** Qual a diferença? Disponível em https:// www.binapratica.com.br/dados-x-informacao. Acesso em 11 de janeiro de 2022.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA - ENAP. **Gestão documental.** Disponível em: https://www.escolavirtual.gov.br/curso/703. Acesso em 12 de maio de 2022.

ERPLAN. **Hierarquia das Medidas de Controle (HMC) indica caminhos para gestão em SST.** Disponível em: https://www.erplan.com.br/noticias/hierarquia-das-medidas-de-controle - hmc-indica-caminhos-para-gestao-em-sst/. Acesso em 13 de fevereiro de 2022.

ESCOLA SUPERIOR DE REDES. **Gestão de riscos de TI: como mitigar riscos das organizações.** Disponível em: https://esr.rnp.br/governanca-de-ti/gestao-de-riscos -de-ti-esr/. Acesso em 14 de setembro de 2021.

EVALTEC. **8 problemas gerados por não ter proteção de dados.** Disponível em; https:// www.evaltec.com.br/8-problemas-gerados-por-nao-ter-protecao-de-dados/. Acesso em 23 de setembro de 2021.

FERNANDES, Jorge Henrique Cabral. **INTRODUÇÃO À GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO.** Disponível em: https://www.trf3.jus.br/documentos/ rget/seguranca/CLRI/GSIC302_Introducao_Gestao_Riscos_Seguranca_Informacao.pdf.Acesso em 21 de janeiro de 2022.

FERREIRA, Sibele Maria Gonçalves. **SISTEMA DE INFORMAÇÃO EM SAÚDE - CONCEITOS FUNDAMENTAIS E ORGANIZAÇÃO.** Disponível em: https://www.nescon.medicina.ufmg.br/biblioteca/imagem/2249.pdf. Acesso em 03 de fevereiro de 2022.

FLEMING, Maria Cristina. **LGPD: diferenças no tratamento de dados pessoais e dados pessoais sensíveis.** Disponível em: https://www.conjur.com.br/2021-mar-06/fleming - diferencas-tratamento-dados-pessoais-sensiveis. Acesso em 02 de outubro de 2021.

GOULART, Guilherme Damasio. **Dados pessoais e dados sensíveis: a insuficiência da informação.** Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/22/18. Acesso em 09 de setembro de 2021.

HINTZBERGEN, Jule et al. **Fundamentos de segurança da informação.** 3. ed. Rio de Janeiro: Brasport, 2018.

LISKA, Allan; GALLO, Timothy. **Ransomware: defendendo-se da extorsão digital.** Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=lang_pt&id= gf6ZDwAAQBAJ&oi=fnd&pg=PT3&dq=ransomware+historia&ots=SF-cHMai1I&sig=LlaP QEbknd32v3pLjA3RBIVzU3s#v=onepage&q&f=false. Acesso em 13 de setembro de 2021.

LOBO, Adilson. **O registro clínico computadorizado**. Disponível em: http://www.periodicosibepes.org.br/index.php/reinfo/article/view/229/137. Acesso em 02 de outubro de 2021.

LORECCHIO, Mariana Martins Ferreira. **O impacto da LGPD nos comércios locais.** Disponível em: https://depaduaadvogados.com.br/Publicacoes/lgpd-comercio-lojas-fisicas/. Acesso em 09 de fevereiro de 2022.

MALWAREBYTES. **PHISHING.** Disponível em: https://br.malwarebytes.com/phishing/. Acesso em 12 de julho de 2022.

MARCONDES, Jose Sergio. **Política de Mesas Limpas e Telas Limpas na Segurança da Informação.** Disponível em: https://gestaodesegurancaprivada.com.br/politica-de-mesas-limpas-e-telas-limpas-na-seguranca-da-informacao/. Acesso em 12 de setembro de 2022.

MARTINS, Guilherme Magalhães; TELES, Carlos André Coutinho. **A telemedicina na saúde suplementar e a responsabilidade civil do médico no tratamento de dados à luz da LGPD.** Disponível em: https://www.estudosinstitucionais.com/REI/article/view/608/670. Acesso em 28 de setembro de 2021.

MAZZO, Bruno Martelli. **A vulnerabilidade da proteção de dados no Brasil: Estamos seguros? Quais os impactos para nossas vidas?** Disponível em: https://mospadvogados.com.br/lgpd/a-vulnerabilidade-da-protecao-de-dados-no-brasil-estamos-seguros-quais-os-impactos-para-nossas-vidas/. Acesso em 09 de outubro de 2021.

MICROSOFT. **Proteja-se contra phishing.** Disponível em: https://support.microsoft.com/pt-br/windows/proteja-se-contra-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44#:~:text=Phishing%20(pronunciado%3A%20fishing)%20%C3%A9,sites%20que%20fingem%20ser%20leg%C3%ADtimos. Acesso em 09 de out. de 2022.

NASCIMENTO, Lucimeiry Maria Minuzzi e; TÓFFOLO, Rosa Maria Machado; TOMAÉL, Maria Inês. **GESTÃO DA INFORMAÇÃO:** do dado à tomada de decisão. Disponível em: http://www.uel.br/eventos/cinf/index.php/secin2011/secin2011/paper/viewFile/23/13. Acesso em 16 de janeiro de 2021.

NEGRI, Sergio Marcos Carvalho de Ávila; Korkmaz, Maria Regina Detoni Cavalcanti Rigolon Korkmaz. **A normatividade dos dados sensíveis na lei geral de proteção de dados:** ampliação conceitual e proteção da pessoa humana. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf. Acesso em 03 de outubro de 2021.

PIEKARSKI, Joseli Inês. **Vulnerabilidade digital de novas tecnologias: técnicas utilizadas através do meio digital que podem ser aplicadas em processo de espionagem e no cybercrime.** Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/3702/1/AD6_ artigo_final_pos_defesa.pdf. Acesso em 02 de outubro de 2021.

SAISSE, Renan Cabral. **Ransomware: "sequestro"de dados e extorsão digital.** Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/44/42. Acesso em 23 de setembro de 2021.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. **A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (LGPD) : Lei.13.709/ 2018** .Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/ 2172/694. Acesso em 22 de setembro de 2021.

SAVELLI, Thiago. **Falhas de segurança digital:** Conheça as 7 mais comuns em PMEs. Disponível em: https://www.psafe.com/blog/falhas-de-seguranca-digital/. Acesso em 02 de janeiro de 2021.

SEMPRO. **LGPD: dados sensíveis.** Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd. Acesso em 08 de setembro de 2021.

SILVA, Ulisses Reis da. **Importância: gerenciamento de risco em TI.** Disponível em: http://www.techoje.com.br/site/techoje/categoria/detalhe_artigo/391. Acesso em 03 de setembro de 2021.

SILVA, Jonathas Luiz Carvalho; GOMES, Henriette Ferreira. **CONCEITOS DE INFORMAÇÃO NA CIÊNCIA DA INFORMAÇÃO:** percepções analíticas, proposições e

categorizações. Disponível em: https://www.brapci.inf.br/_repositorio/2015/12/pdf_22d51b99a9_0000007714.pdf. Acesso em 07 de janeiro de 2022.

SILVEIRA, Suzana Aparecida. **Segurança da informação e proteção de dados pessoais:** estudo de caso e proposta de governança para serviços de saúde. Disponível em: https://repositorio.unifesp.br/bitstream/handle/11600/60909/Defesa%20MPIT%20SUZANA%20APARECIDA%20SILVEIRA%20VERSA%cc%83O%20FINAL%20UNIFESP%20CBM.pdf?sequence=1&isAllowed=y. Acesso em 05 de setembro de 2021.

SOARES, Flaviana Rampazzo. **Consentimento no direito da saúde nos contextos de atendimento médico e de LGPD:** diferenças, semelhanças e consequências no âmbito dos defeitos e da responsabilidade. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc /article/view/170/135. Acesso em 02 de outubro de 2021.

UNIVERSIDADE FEDERAL DO SUL E SUDESTE DO PARÁ - UNIFESSPA. **Procedimentos para Eliminação de Documentos.** Disponível em: https://arquivocentral.unifesspa.edu.br/ eliminacao-de-documentos.html. Acesso em 21 de julho de 2022.

ZIMMER, Kelvin. **Como funciona o golpe de e-mail falso?** Disponível em: https://www.lumiun.com/blog/como-funciona-o-golpe-de-e-mail-falso/. Acesso em 12 de agosto de 2022.

APÊNDICE

APÊNDICE A - Seções da ISO 27001 aplicada a cenário médico fictício

Seção	Descrição	Exemplo
4 - Contexto da organização	Entender a organização e seu contexto 4.2.Entendendo as necessidades e as expectativas das partes interessadas 4.3. Determinando o escopo do sistema de gestão da segurança da informação	● Análise de estrutura da clínica ● Análise das responsabilidades ● Análise de processos médicos ● Análise de relações e partes interessadas
5 - Liderança	5.1 Liderança e comprometimento 5.2 Política 5.3 Autoridades, responsabilidades e papéis organizacionais	● Estabelecer responsabilidades e autoridades para a segurança da informação dos dados sensíveis. ● Estabelecimento de políticas na clínica.
6 - Planejamento	6.1 Ações para contemplar riscos e oportunidades 6.1.2 Avaliação de riscos de segurança da informação 6.1.3 Tratamento de riscos de segurança da informação. 6.2 Objetivo de segurança da informação e planejamento para alcançá-los	● Tratamento dos riscos ● Planejamentos para combater riscos.
7 - Apoio	7.1 Recursos 7.2 Competência 7.3 Conscientização 7.4 Comunicação 7.5 Informação documentada	● Recursos financeiros, documentais, etc. ● Treinamento aos colaboradores ● Comunicação aos colaboradores
8 - Operação	8.1 Planejamento operacional e controle 8.2 Avaliação de riscos de segurança da informação 8.3 Tratamento de riscos de segurança da informação	● Realização da análise de risco da clínica. ● Implementação do plano de tratamento de riscos
9 - Avaliação de desempenho	9.1 Monitoramento, medição, análise e avaliação 9.2 Auditoria interna 9.3 Análise crítica pela Direção	● Testar e monitorar o desempenho das técnicas escolhidas para a segurança dos dados sensíveis. ● Realização de análise crítica.
10 - Melhoria	10.1 Não conformidade e ação corretiva 10.2 Melhoria contínua	● Melhorias e correções para os métodos escolhidos de segurança da informação.

APÊNDICE B - Controle de risco - Clínica Med&Clinic

	Tipo de ativo	Setor localizado	Classificação	Vulnerabilidades apresentadas	Controles sugeridos
Anotações /lembretes e recados simples Modelos de relatórios	Ativo físico ou digital	Setores diversos	Interno	● Documentação exposta em mesas, balcões, quadros ou impressoras. ● Eliminação incorreta de documentos. ● Visualização de fichas em computadores com seções abertas. ● Setores e salas com fácil acessibilidade.	● Política de mesa limpa ● Eliminação correta dos documentos ● Acesso restrito a documentos
Fichas de cadastro Contratos organizacionais Currículos, fichas de colaboradores	Ativo físico ou digital	Recepção, triagem, Financeiro Administrativo, RH.	Restrito		
Relatório médico Receituário	Ativo físico ou digital	Consultório médico arquivo médico	Confidencial		
Servidores e seus tipos: Firewall, antivírus, arquivos, web	Ativo físico	TI	Confidencial	● Acesso facilitado a sala ● Falhas de backup ● Falhas de manutenção (proteção contra incêndios, falhas elétricas e derivados) ● Falhas de operação (Portas abertas no firewall, falhas em atualizações e senhas frágeis)	● Atualizações de software ● Antivírus ● Proteção de portas Firewall ● Restrição de acesso físico a sala ● Proteção contra desastres naturais
Salas e controles físicos	Ativo físico	Setores diversos	Público Interno Restrito Confidencial	● Falta de dispositivos e métodos relacionados à manutenção e proteção de ativos: extintores, sprinkler e desumidificadores	● Proteção contra desastres naturais e agentes biológicos ● Restrição de acesso às salas
SGSSO e outros softwares de gestão	Ativo digital	TI (servidores)	Interno ou restrito (de acordo ao acesso dentro do software)	● Senhas fáceis, ● Falhas de autorização e criptografia, disponibilidade e backup ● Falha de autenticação	● Proteções criptográficas ● Backup seguro ● Verificação em duas etapas ● Autenticação ● Login com senhas fortes

APÊNDICE C - Exemplo de termo de compromisso para coleta de dados sensíveis

Eu _____Portador(a) do CPF_____ e RG_____, Natural do município de_____ , residente e domiciliado à_____ declaro que autorizo a clínica **NOME DA CLÍNICA**, definida aqui como controladora de dados a dispor dos meus dados pessoais e sensíveis, de acordo ao artigo 7° e 11° da Lei geral de proteção de dados (LGPD - 13.709), conforme termos descrito:

1 - O titular autoriza que a clínica **NOME DA CLÍNICA** utilize seus dados para as seguintes finalidades:

DESCREVER FINALIDADES

2- A clínica **NOME DA CLÍNICA** fica autorizada a compartilhar os dados com outros agentes, conforme seja necessária a finalidade, priorizando o respeito e sigilo médico, utilizando desse compartilhamento apenas para finalidades descritas:

DESCREVER FINALIDADES.

3- A clínica **NOME DA CLÍNICA** se responsabiliza por manter ações de segurança, priorizando a proteção dos dados sensíveis, comunicando ao titular a ocorrência de algum incidente, conforme artigo 48° da lei 13.709.

4- É garantido ao titular a entrada de acordo, quando ocorrerem eventos danosos aos dados, como vazamentos ou acessos não autorizados, e a controladora tem ciência que estará sujeita a penalidades na ocorrência dos eventos citados anteriormente, conforme artigo 52°da lei 13.709.

_____

ASSINATURA DO TITULAR

ANEXOS

ANEXO A - Categorias do controle de risco conforme ISO/ABNT 27701/27001

Grau dos requisitos	Tipos	Descrição
Mínimos	Conscientização	Criar, revisar e comunicar diretrizes para segurança.
	Controle de acesso	Acessos a dados e logins somente as pessoas autorizadas e revogar a disponibilidade para pessoas que sairam da organização.
	Backups	Garantir cópias de segurança devidamente protegida contra acessos não autorizados.
	Ativos	Inventariar os ativos que tratam dados pessoais
	Segurança End-point	Garantir que os ativos possuam soluções de antimalware instalada e atualizada periodicamente.
Prioritários	Monitoramento de incidentes	Monitorar o comportamento dos acessos e da segurança dos ativos envolvidos no tratamento dos dados.
	Log de sistema	data, horário, duração, identidade do funcionário/ responsável pelo acesso e a ação executada.
	Controle de vazamento	Prevenir o vazamento dos dados pessoais.
	Segurança física	Garantir a segurança do acesso físico como mídias eletrônica, papel e sistemas.
	Gestão de vulnerabilidade	Avaliar e executar testes de segurança nos sistemas que tratam dados pessoais.
Avançados	Arquitetura de segurança	Analisar e identificar melhorias para a proteção dos dados pessoais envolvendo a arquitetura de tecnologias.
	Transferência de Dados	Garantir a segurança na comunicação durante os processos de transferências de dados.
	Exclusão de Dados	Mapear a localização dos dados pessoais para que possam ser excluídos quando solicitado.
	Mascaramento	Avaliar o uso de mascaramento de dados quando aplicável.
	Pseudoanonimização	Avaliar o uso de pseudo-anonimização quando aplicável.
	Desenvolvimento seguro	Avaliar se o produto/sistema desenvolvidos estão integrados conforme as implementações e requisitos de segurança.
	Criptografia	Avaliar a aplicação de recursos de criptografia de dados pessoais quando necessária.

Fonte: CONFEDERAÇÃO NACIONAL DA SAÚDE. **Código de boas práticas:** proteção de dados para presta dores privados em saúde. Visto em: http://cnsaude.org.br/wp-content/uploads/2021/03/ Boas-Praticas-Protecao-Dados- Prestadores-Privados- CNSaude_ED_2021.pdf. Acesso em 12 de fevereiro de 2022.