TÉCNICO LISBOA

Avaliação do Risco Intrínseco de Ativos

Estudo de caso do impacto Covid-19

Luísa Alexandra Inácio Varandas dos Santos

Dissertação para obtenção de grau de Mestre em Segurança de Informação e Direito no Ciberespaço

Mestrado em Segurança de Informação

e Direito no Ciberespaço

Supervisão

Professor Doutor Anacleto Cortez e Correia

Professor Capitão-tenente Mário Rui Monteiro Marques

Professor Doutor Carlos Caleiro

Júri

Professor Doutor Paulo Alexandre Carreira Mateus

Professor Doutor Victor José de Almeida e Sousa Lobo

Professor Doutor Anacleto Cortez Correia

outubro/2021

Epígrafe

"Mesmo quando baseada numa análise meticulosa, dotada de uma definição clara da área de atuação e conscienciosamente gerida, a inovação com base em novos conhecimentos sofre ainda de riscos únicos e, pior do que isso, de uma impressibilidade inata."
[1]

"Todas as outras inovações exploram uma mudança já efetuada. Satisfazem uma necessidade já existente. Mas no caso da inovação baseada em novos conhecimentos, é a inovação que provoca a mudança. É ela que pretende criar uma necessidade. E ninguém pode dizer de antemão se o utilizador lhe será receptivo, indiferente, ou se lhe oporá uma resistência activa"
[1]

Dedicatória

Aos meus pais por me acompanharem em todas as jornadas da minha vida, académicas, profissionais e pessoais.

Agradecimentos

Quando iniciei o desafio académico de me candidatar ao Mestrado Integrado de Segurança de Informação e Direito no Ciberespaço (MSIDC), no final de 2018, encontrava-me também, em fase de mudanças profissionais.

O primeiro ano curricular foi exigente, no entanto toda a disponibilidade e conhecimento partilhado pelos professores do Instituto Superior Técnico (IST), Faculdade de Direito da Universidade de Lisboa (FDUL) e Escola Naval do Alfeite (EN), permitiram que os meus objetivos académicos fossem cumpridos, mas não só, também o conteúdo programático das unidades curriculares do primeiro ano de mestrado, contribuiu para amadurecer a ideia que tinha para o âmbito da dissertação a desenvolver no 2º ano de mestrado. Foi, aliás, decisivo o artigo cientifico publicado na revista cientifica CIBERLAW, do Centro de Investigação de Direito do Ciberespaço da Faculdade de Direito da Universidade de Lisboa (CJIC), em maio de 2019, elaborado em contexto académico sobre a supervisão do professor Capitão-tenente Mário Rui Monteiro Marques, que me permitiu definir exatamente o âmbito da dissertação deste mestrado, i.e., Análise de Risco Aplicada à Segurança de Informação, especificamente a fase de avaliação do risco intrínseco de Ativos [2].

O segundo ano, muito mais exigente se tornou, com novos desafios profissionais e um estado pandémico a nível mundial, Covid-19, que alterou rotinas e formas de trabalho, evidenciando a necessidade de implementação de metodologias de gestão de risco organizacional aplicado à Segurança de Informação, pela maior parte das organizações publicas e privadas.

Iniciei assim, uma jornada de investigação na Autoridade Nacional de Segurança Rodoviária (ANSR), organismo público onde me encontro atualmente a Coordenar um Núcleo de Informática (NIF), que me permitiu caracterizar um Caso de Estudo específico, para a presente dissertação de mestrado.

Face a todo este enquadramento, tenho a agradecer, em primeiro lugar, ao professor da EN, Capitão-tenente Mário Rui Monteiro Marques por me ter ajudado a definir o tema da dissertação, enquadrando o mesmo com o artigo científico publicado em 2019, sob a sua orientação.

Agradeço também ao professor da EN, Doutor Anacleto Cortez e Correia, pela disponibilidade demonstrada e admirável assertividade, na orientação da dissertação e, especialmente, por me ter apoiado no foco e construção da estrutura da mesma.

Ainda a nível académico, não posso deixar de referenciar e muito agradecer, o precioso apoio do professor do IST, Doutor Carlos Caleiro, Coordenador do MSIDC, que sempre promoveu e conciliou, a ligação dos mestrandos com o corpo docente, o que mitigou muitos dos constrangimentos do mestrado, advindos da complexidade de envolvimento de três entidades do ensino superior, tão destintas e diferenciadas, o IST, a EN e a FDUL.

Por outro lado, mas não menos importante, a concretização desta dissertação e investigação para o âmbito da mesma, foi um esforço complexo, em contexto de trabalho, tenho, por isso a agradecer toda a compreensão de quem me recebeu num novo desafio profissional, sempre com a disposição de conciliação entre as exigências académicas e profissionais. Agradeço muito, por isso, ao Sr. Presidente da ANSR Professor Doutor Rui Ribeiro e à Sr.ª Vice-presidente Eng.ª Ana Tomaz, por me terem proporcionado o acesso a dados para a investigação e autorizado o uso dos mesmos para efeitos académicos, ao Dr. Nuno Santos, Chefe da Divisão onde o NIF se insere, por sempre me ter apoiado e incentivado neste percurso académico.

Agradeço também, à Rede Nacional de Segurança Interna (RNSI), nomeadamente ao Sr. Secretário-geral Adjunto Dr. António Pombeiro e ao Sr. Diretor de Serviço de Tecnologias de Informação e Comunicação Dr. Vítor Costa, por me terem disponibilizado os dados para a investigação.

Deixo para ultimo, aqueles a quem devo um agradecimento muito especial, assim, é com muita estima e reconhecimento, que agradeço à minha equipa de trabalho, o Núcleo de Informática, da Divisão de Apoio e Desenvolvimento Organizacional, da ANSR, por toda a colaboração e lealdade que me têm prestado, e acima de tudo por me terem proporcionado o tão valioso tempo, para que me dedicasse à construção desta dissertação de mestrado.

Estou muito grata a todos!

Resumo

Em meados de março de 2020, houve uma preocupação única e transversal a todo o setor público e privado no Pais, em reduzir ao máximo o número de contágios por Covid-19. A ANSR, deparou-se com uma pandemia mundial, obrigando a mudanças “inovações” relativas às rotinas e modalidades de trabalho atuais, promovendo a realidade teletrabalho.

Esta nova realidade, o teletrabalho, resultou também numa vulnerabilidade, como potencial fator acentuador da concretização de determinadas ameaças à Segurança de Informação da ANSR.

Foram, assim, recolhidas evidências das circunstâncias atuais, durante o primeiro semestre do ano de 2020, para puderem ser observadas, no sentido de aperfeiçoar o objetivo desta dissertação: apurar o risco intrínseco dos ativos em modalidade de teletrabalho da ANSR, em contexto pandemia Covid-19, face aos eventos apurados de ameaças e vulnerabilidades entre janeiro de 2019 e julho de 2020, através de um modelo de gestão de risco integrado, pelas normas ISO31000 e ISO27005.

Palavras Chave: Risco, Segurança de Informação, Vulnerabilidades, Ameaças.

Abstract

In mid-March 2020, there was a unique and transversal concern to the entire public and private sector in Portugal, reducing the number of contagions by Covid-19 as much as possible. ANSR, faced with a worldwide pandemic, forcing changes "innovations" related to current routines and work modalities, promoting the reality Telework.

This new reality, Teleworking, has also resulted in a vulnerability, as a potential factor that accentuates the action of certain threats to ANSR's Information Security.

Therefore, evidence of the current circumstances was collected, during the first half of the year 2020, that could be observed, in order to ascertain the objective of this dissertation: to ascertain the intrinsic risk of ANSR's teleworking assets, in a Covid-19 pandemic context, in the light of the events of threats and vulnerabilities between January 2019 and July 2020, through the risk assessment phases of an integrated risk management model, according to ISO31000 and ISO27005 standards.

Keywords: Risk, Information Security, Vulnerabilities, Threats.

Índice

índice Tabelas

Índice Figuras

Lista de abreviaturas, siglas e acrónimos

ANACOM – Autoridade Nacional de Comunicações

ANSR – Autoridade Nacional de Segurança Rodoviária

BPM *- Business Process Management*

CERT.PT - Centro Nacional de Respostas a Incidentes do CNCS

CCD – Centro de Ciberdefesa

CIRC - *Computer Incident Response Capability*

CJIC – Centro de Investigação de Direito do Ciberespaço da Faculdade de Direito da Universidade de Lisboa

CNCS – Centro Nacional de Cibersegurança

COBIT *- Control Objectives for Information and related Technology*

DADO - Divisão de Apoio e Desenvolvimento Organizacional

EN – Escola Naval

ENISA - *European Union Agency for Cybersecurity*

FDUL – Faculdade de Direito da Universidade de Lisboa

IPAC – Instituto Português de Acreditação

ISACA *- Information Systems Audit and Control Association*

ISO *- International Organization for Standardization*

IST – Instituto Superior Técnico de Lisboa

ITIL *– Information Technology Infrastructure Library*

MAI – Ministério da Administração Interna

MDN - Ministério da Defesa Nacional

MSIDC – Mestrado Integrado de Segurança de Informação e Direito no Ciberespaço

NIF – Núcleo de Informática da ANSR

NCIRC - *NATO Computer Incident Response Capability*

OMS - Organização Mundial de Saúde (OMS)

RGPD – Regulamento Geral de Proteção de Dados UE 2016/679

RNID - Regulamento Nacional de Interoperabilidade Digital UE 2016/1148

RNSI – Rede Nacional de Segurança Interna do Ministério da Administração Interna

SGSI - Sistema de Gestão de Segurança de Informação

SGSTI - Sistema de Gestão de Serviços TI

SoE *– Social Engineering*

SI - Sistema de Informação

TI - Tecnologias de Informação

CAPÍTULO I - Introdução

O presente capítulo, aborda o enquadramento da dissertação, as motivações para a elaboração da mesma, descreve o problema a abordar, bem como, o objetivo que se pretende atingir e a metodologia de investigação proposta para a realização da dissertação. No final do capítulo descreve-se a estrutura da dissertação.

1. Enquadramento

A revolução tecnológica iniciada nas últimas décadas do sec. XX, transformou todo o conceito ***Informação***. As organizações assistiram a uma mudança de paradigma em que, este ativo, a Informação, deixou se ser algo apenas físico, tornou-se num ativo essencialmente digital.

O que antes já era alvo de ameaças como por exemplo espionagem industrial, i.e., informação em formato físico, de valiosíssimo valor para as suas organizações, que eram acedidos por origens não autorizadas, através de meios e para fins ilícitos, passa a ter uma maior complexidade na sua proteção, observando que a mesma ao tornar-se digital, aumenta toda a complexidade de a proteger de acessos ilícitos, isto porque a sua reprodução e divulgação tornam-se muito mais dinâmicas.

A informação na era digital, deixa de ser um alvo de fácil identificação a proteger, em que muitas das vezes, a proteção deste ativo, passa por avaliar e gerir o risco da possibilidade da mesma ser acedida por destinos não autorizados, ou da sua perda total ou parcial. As organizações passam assim a evidenciar particular preocupação na proteção deste ativo, organizações estas com, ou sem um foco estritamente empresarial e comercial como, por exemplo organizações que têm um foco regulador e fiscalizador de um setor específico, como é caso da Autoridade Nacional de Segurança Rodoviária (ANSR).

Para compreendermos o âmbito da presente dissertação, será necessário perceber, sobre que dimensões no ciberespaço poderá ter impacto, a ausência de uma avaliação de risco intrínseco de Ativos, numa organização, face a ameaças e vulnerabilidades a esses Ativos. Entende-se por Ciberespaço toda a envolvente multidimensional territorial, tecnológica, sociológica, jurídica, política, estratégica e de segurança, decorrente da utilização de infraestruturas de tecnologias de informação.

Dentro do ciberespaço, podem ocorrer ciberataques, i.e., ataques com o objetivo de atingir infraestruturas de tecnologias de informação, podendo estes, ser direcionados à população em geral ou à soberania de estados. Associada à motivação dos ciberataques podem ocorrer interações preventivas e corretivas de segurança, em duas dimensões, na **Cibersegurança** que resulta na ação por parte de um Estado Soberano com o objetivo de zelar pela segurança dos seus cidadãos enquanto utilizadores do Ciberespaço e na **Ciberdefesa** que interage do mesmo modo mas acautelando a defesa da soberania do próprio Estado Soberano [3]. A conjunção destas duas dimensões, Cibersegurança e Ciberdefesa, define-se como **Cibersegurança Nacional** ilustrada na Figura 1 [4].

Figura 1 - Enquadramento da Cibersegurança Nacional pelo Instituto de Defesa Nacional Fonte: [4]

Neste âmbito, realça-se a importância de que, a ausência de uma avaliação de risco intrínseco dos Ativos de determinada organização, face às mais variadas ameaças e vulnerabilidades a que esses Ativos possam estar sujeitos, poderá colocar em causa não apenas a continuidade de negócio das organizações, mas também, a própria **Cibersegurança Nacional**.

Em março de 2020, os e-mails de *phishing* tinham aumentado em mais de 600% desde o final de fevereiro desse mesmo ano, à medida que os cibercriminosos foram explorando o medo e a incerteza gerados pela pandemia COVID-19. Dos 468.000 ataques globais detetados via e-mail, no ano 2020, cerca de 2% foram relacionados com o tema COVID-19, em que foram registados: em janeiro 137 incidentes; em fevereiro 1.188 e em março 9.116. Da observação a estes ataques, resultou que 54% foram classificados como fraudes e golpes, 34% como ataques de falsificação de identidade de marca, 11% como chantagem e 1% como comprometimento de e-mail corporativo [5].

Em abril de 2020 um inquérito, a 1300 responsáveis de segurança de informação de várias organizações internacionais, onde se pretendeu recolher dados relativamente à evolução do cibercrime e o incremento do risco, em contexto de pandemia Covid-19 e teletrabalho, evidenciava que 59% das organizações inquiridas reportaram um aumento de ataques destrutivos em 2020, ou seja, em plena pandemia Covid-19, sendo que, 34% da origem mais comum desses ataques é de colaboradores internos da organização ou de parceiros de negócio (18% colaboradores com pouca literacia em segurança digital, 10% colaboradores mal-intencionados e 8 % parceiros ou fornecedores) e o principal alvo dos ataques são dados de clientes das organizações (45% dados de clientes) [6]

O Centro Nacional de Cibersegurança (CNCS) referenciou um aumento de Ciberataques verificado nesse mesmo mês de 2020, destacando que contextos internacionais de crise, como no caso da pandemia mundial Covid-19, são normalmente explorados por indivíduos hostis do Ciberespaço. Sobre o tipo de Ciberataques, o CNCS apontava o *phishing* como um dos mais preocupantes, i.e., ataques que têm como objetivo manipular um determinado utilizador, usando o nome de uma entidade de confiança, através de e-mail, chamada telefónica ou de um serviço on-line, para obter dados sensíveis tais como: palavras-chave, números de cartões de crédito, entre outros. Apontava também

o CNCS, que este tipo de ataques é mais evidente em contexto organizacional, do setor público e privado, sendo estas as entidades que mais notificações de ataques reportam ao CNCS. Estas informações do CNCS, ocorrem no mês imediatamente seguinte ao estado de emergência, declarado pelo Governo Português, que fez com que as organizações do setor privado e publico, colocassem os seus colaboradores maioritariamente em regime de teletrabalho [7], [8].

Em maio de 2020, a *European Union Agency for Cybersecurity* (ENISA), indicava que os ataques de *phishing*, via e-mail, aumentaram em contexto pandémico Covid-19, e que estes ataques, via e-mail, recorrem a formas fraudulentas de apropriação de imagem de determinadas organizações credíveis, governamentais, ministérios da saúde, centros de saúde pública ou figuras importantes de um país, com o propósito de se disfarçarem de fontes confiáveis, aos seus alvos, utilizadores no Ciberespaço. A *ENISA*, referenciava que este aumento estaria interligado com o facto de muitas organizações e empresas terem adaptado as suas condições de trabalho devido à pandemia COVID-19, promovendo o aumento de atividades remotas, como o teletrabalho, e que este, aumenta a dependência do e-mail para comunicação, criando assim condições perfeitas para esquemas de fraude por e-mail [9].

O CNCS publicou o Relatório Cibersegurança em Portugal – Sociedade, do Observatório de Cibersegurança, que aponta para um crescimento significativo do número de incidentes registados pelo Centro de Respostas a Incidentes do CNCS (CERT.PT), em cerca 101%, quando comparados entre o primeiro semestre de 2019 e o primeiro semestre de 2020, em que destes 101% de incidentes, o *phishing*, foi o mais frequente correspondendo a 36% dos incidentes registados. Assim, pese embora o relatório incida maioritariamente sobre dados de 2019, é possível retirar conclusões do estado pandémico Covid-19, associando o mesmo ao aumento de ciberameaças relacionadas com campanhas de *phishing*, entre outras, para o primeiro semestre de 2020 em comparação com o período homólogo anterior, invocando preocupações relacionadas com a pandemia Covid-19, que podem ter impacto nos indicadores representados e relativos a 2019, tais como [10]:

- Dados da Autoridade Nacional de Comunicações (ANACOM), indicam que o aumento em 61,1% do consumo do serviço de Internet fixa, no primeiro semestre de 2020, comparando com o período homólogo do ano anterior (ANACOM, 2020);

- O facto do aumento do consumo do serviço de internet entre 2019 e 2020, poder estar relacionado com as alterações na organização do trabalho, bem como, noutras áreas (ensino, transportes, entre outros) consequência do estado pandémico vivido atualmente e espoletado no início de 2020, que provocou uma maior dependência dos serviços digitais e consequentemente do uso mais frequente de equipamentos de mobilidade (computadores, dispositivos moveis, etc) dentro ou fora do contexto organizacional.

No Relatório Cibersegurança em Portugal – Sociedade, do Observatório de Cibersegurança, publicado em dezembro de 2020, pelo CNCS, ressalva-se que, ainda que não seja possível identificar

consequências da pandemia Covid-19, ainda assim, existe o alerta para o baixo nível de preparação dos indivíduos e das organizações para as Ciberameaças que acompanharam a pandemia. O relatório destacou indicadores sobre o fator humano ligado à Cibersegurança, muito focado em contexto organizacional, articulando conclusões das análises desses indicadores com a atual pandemia e como todo este contexto se relaciona com as ameaças no Ciberespaço. Evidencia-se entre outros aspetos o aumento de ataques *phishing* a pessoas isoladas em trabalho à distância (teletrabalho) com recurso a técnicas de engenharia social [10].

2. Motivação

Em resultado da pandemia Covid-19 e das recomendações da OMS, as organizações, dos setores público e privado, a nível mundial, colocaram quase toda a totalidade dos seus colaboradores, em regime de teletrabalho, i.e., com a prestação laboral a ser realizada, embora mantendo a subordinação jurídica, fora da organização, através do recurso a tecnologias de informação e de comunicação [11] [12]. Associadas a esta realidade revelam-se vulnerabilidades exploradas por indivíduos mal-intencionados, que promovem ameaças (ataques) através de meios digitais, às organizações, através de os seus colaboradores internos, muitas vezes explorando a iliteracia destes em âmbitos de Segurança de Informação de Tecnologias de Informação ou estados psicossociais dos mesmos. Esta situação acentuou-se num contexto em que muitas organizações se depararam, implementar novas modalidades de trabalho, disponibilizando alternativas fora das instalações físicas das organizações, em regime de teletrabalho.

A ANSR deparou-se com o seu nome a ser utilizado, para promover uma avalanche de ataques *phishing*, através do envio de e-mails fraudulentos, por indivíduos mal-intencionados, para vários cidadãos [13]–[15]. Simultaneamente, registou-se um aumento de incidentes de segurança de informação, no período entre janeiro de 2020 e julho de 2020 face ao período homólogo do ano anterior, sendo o principal fator diferenciador de alteração organizacional, no referido período, a colocação massiva dos seus colaboradores em regime de teletrabalho no início de 2020.

3. Definição do Problema

Em resultado do contexto vivido no estado de emergência, originado pelo pico pandémico Covid-19, foram várias as evidências de crescimento de incidentes de Segurança de Informação, reportados por entidades nacionais e internacionais. Esta dissertação pretende contribuir para a avaliação e monitorização do risco de Segurança de Informação, no contexto das novas formas de organização do trabalho.

A motivação da presente dissertação situa-se no domínio da Análise e Gestão de Risco de Segurança de Informação aplicado a organizações. Pretende assim, validar as conclusões de várias entidades, nacionais e internacionais, no domínio da Segurança de Informação, em contexto pandemia Covid-19, analisando a ANSR, relacionando o teletrabalho em contexto pandemia Covid-19, e o aumento de eventos de ameaças de Segurança de Informação às organizações.

4. Objetivo

O ***objetivo*** da presente dissertação é propor e validar um modelo de gestão de risco de Segurança de Informação adaptado a novas formas de organização do trabalho, que permita apurar o risco intrínseco de determinadas vulnerabilidades e ameaças, às organizações nesse contexto.

A questão principal de investigação colocada é:

> ***Como avaliar e monitorizar o risco para a Segurança de Informação das novas formas de organização do trabalho?***

Da procura de resposta à questão principal, resulta a necessidade de obtenção de respostas às seguintes questões secundárias:

1) Qual o modelo adequado para avaliar e monitorizar o risco para a Segurança de Informação?
2) Qual o método a usar na aplicação do modelo ao Caso de Estudo?
3) Como apurar o risco para a Segurança de Informação das organizações?

5. Metodologia de Investigação

A metodologia utilizada para a investigação será a de Caso de Estudo, aplicado a uma organização do setor público português, a ANSR, permitindo apurar o risco intrínseco dos ativos colocados em regime de teletrabalho, no contexto pandémico Covid-19 [16].

A metodologia de Caso de Estudo, residirá numa perspetiva qualitativa, i.e., será orientada para a análise de um grupo restrito de dados, e avaliação do risco intrínseco através da aplicação de um modelo de gestão de risco, sobre esses dados, com base em eventos diários observados num contexto (pandemia Covid-19) entre janeiro de 2019 e julho de 2020, de determinada organização, que permitirá criar uma relação dos eventos observados com o estado pandémico e outros estudos científicos realizados, para que os fenómenos possam ser compreendidos. Assim, para a caracterização do Caso de Estudo, iremos abordar especificamente a adaptação e utilização das seguintes fases representadas na Figura 2:

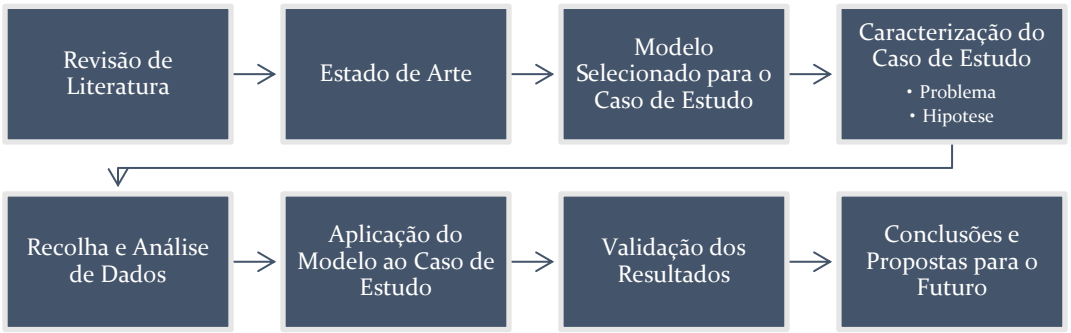

Figura 2 – Fases de Metodologia do Caso de Estudo

Na fase **Revisão da Literatura**, serão descritas as orientações bibliográficas que delimitaram o âmbito do Caso de Estudo e que contribuíram para a análise do mesmo, bem como, a mesma ajudou a definir o tema da dissertação. Na fase **Estado de Arte**, serão observados os modelos mais relevantes, em contexto organizacional, no âmbito de avaliação de risco intrínseco de Ativos, relativamente à Segurança de Informação de Tecnologias de Informação.

Na fase *Seleção do* **Modelo para o Caso de Estudo**, será indicado, com base nos modelos observados, qual o Modelo de Avaliação de Risco Intrínseco de Ativos, a utilizar para aplicar sobre o caso de estudo, respondendo à questão secundária **1)** do ponto 4 do presente capítulo. Na fase **Caracterização do Caso de Estudo,** será identificado o Problema e formulação da Hipótese ao mesmo, tendo em conta a realidade analisada, i.e., caso específico de uma organização do setor público português, sempre com a perspetiva de demonstrar uma solução aplicável a qualquer organização independentemente do setor em que se insere e da sua nacionalidade. Na fase **Aplicação do Modelo ao Caso de Estudo**, iremos aplicar o modelo de Avaliação de Risco Intrínseco de Ativos sobre o Caso de Estudo, respondendo à questão secundária **2)** do ponto 4. do presente capítulo.

Na fase **Recolha e Análise de Dados**, indicar-se-ão as fontes de recolha dos dados, os ajustamentos aos mesmos no enquadramento do Caso de Estudo e a análise qualitativa e quantitativa dos mesmos. Na fase **Validação dos Resultados**, serão validados os resultados, indicando de que forma responde à questão secundária **3)** do ponto 4. do presente capítulo. Na fase **Conclusões e Propostas para o Futuro**, serão abordadas as conclusões finais da dissertação e propostas para o futuro no âmbito da mesma, e dada resposta à questão principal do ponto 4. do presente capítulo.

6. Estrutura da Dissertação

A dissertação subdivide-se em sete capítulos. De acordo com a Figura 3, o ***primeiro capítulo - Introdução -*** foca-se no enquadramento da dissertação, dando uma visão geral da mesma e enfâse ao tema científico que se pretende abordar, bem como, indica as motivações para o trabalho de investigação, o objetivo e a metodologia seguida. O ***segundo capítulo - Contexto -*** demonstra a pesquisa de literatura e documentos consultados para a investigação do tema, faz também uma abordagem ao estado de arte relativamente ao contexto da dissertação apresentada, propondo e validando um modelo de gestão de risco de Segurança de Informação adaptado a novas formas de organização do trabalho, sobre o qual se focará a presente dissertação. O ***terceiro capítulo – Metodologia Proposta para a Avaliação de Risco e Segurança –*** faz a apresentação da metodologia seguida, de um ponto de vista geral, e a aplicabilidade de mesma a qualquer tipo de organização. O ***quarto e quinto capítulos - Caso de Estudo -*** demonstram a caracterização do caso de estudo através da colocação do problema e hipótese ao mesmo, apresenta a recolha e análise dos dados tratados para o caso de estudo e representa a aplicação do modelo. No ***sexto capítulo - Resultados -*** pretende-se demonstrar a validação dos dados. O ***sétimo capítulo - Conclusões -*** apresenta as conclusões da dissertação.

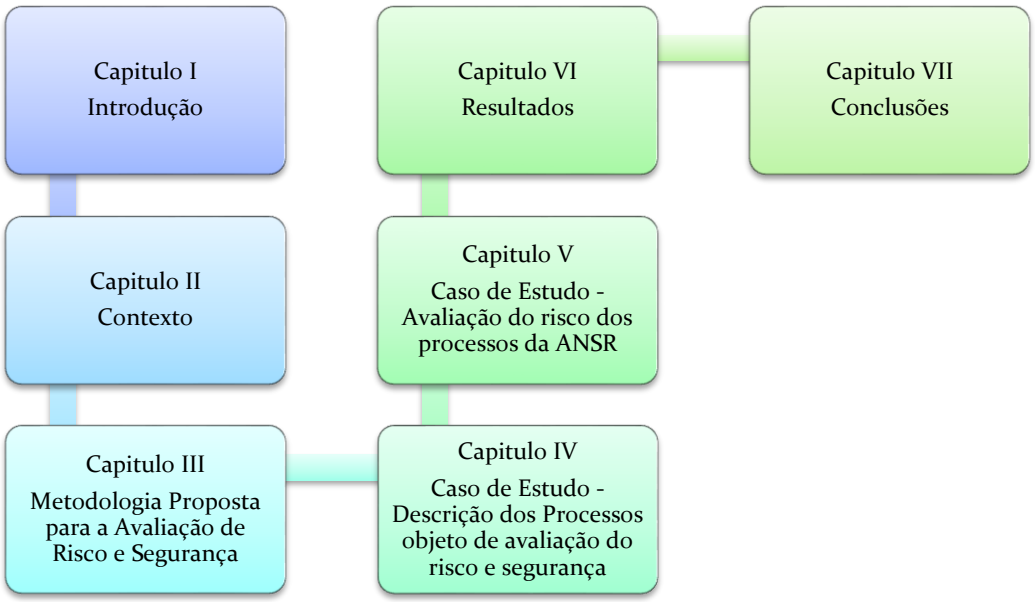

Figura 3 – Estrutura da Dissertação

CAPÍTULO II - Contexto

1. Revisão da Literatura

A pesquisa de literatura focou-se no domínio da Gestão de Risco de Segurança de Informação em Serviços de Tecnologias de Informação, tendo em conta os novos desafios no domínio da cibersegurança, em contexto organizacional e novas formas de trabalho em período pandémico. Nas pesquisas realizadas, foram usadas as palavras chave: gestão de risco, ameaça, vulnerabilidade, Segurança de Informação, teletrabalho, stresse, ansiedade, Covid-19, cibersegurança.

contribuiu também para dissertação a legislação em vigor, quer a nível nacional quer a nível europeu, com o foco na Segurança das Redes e da Informação, Interoperabilidade Digital e Privacidade de Dados Pessoais , respetivamente: Diretiva UE 2016/1148 [17], RNID - Regulamento Nacional de Interoperabilidade Digital [18] e Regulamento Geral de Proteção de Dados (UE) 2016/679 [19], verificando que todas estas referências promovem quer a adoção de processos de gestão de Segurança de Informação, quer de processos de análise e gestão de risco nesse âmbito, no entanto não é clara nem obrigatória a indicação de qual o modelo a adotar pelas organizações, deixando a cargo destas a seleção da metodologia a utilizar.

Relativamente aos contributos científicos e as fontes consultadas para a recolha desses contributos, apresenta-se infra, uma descrição como cada um, em termos de relevância, numa escala de 0-Nenhuma a 5-Muita:

1. *Gestão de risco aplicada à Segurança de Informação* [2]. Modelo conceptual de gestão de risco aplicada à Segurança de Informação. através da implementação de um modelo baseado na norma ISO31000. O modelo demonstra uma metodologia qualitativa e quantitativa, de modo a apurar o risco de determinadas ameaças Vs. vulnerabilidades, face ao impacto destas sobre a segurança de informação. **Relevância**: 5

2. *Resultados Preliminares sobre o impacto Psicossocial da Covid-19 em Portugal* [20]. O Relatório analisa o impacto da pandemia, no comportamento individual e relacional de indivíduos, representando o aumento da sintomatologia de doenças do foro psíquico, durante o isolamento social decorrente da pandemia Covid-19. **Relevância**: 5

3. *Prioridades multidisciplinares de pesquisa para a pandemia Covid-19: um apelo à ação para a ciência da saúde mental* [21]. Estudo científico que evidencia consequências do isolamento social, no período da pandemia Covid-19, na saúde mental e física da humanidade, apontando não só para um incremento de doenças psíquicas em indivíduos que não padeciam destas doenças antes do isolamento social, mas também do agravamento das mesmas em indivíduos que já estavam identificados clinicamente com doenças do foro psíquico (ansiedade, depressão, stress, etc,). **Relevância**: 5

4. *AVARCIBER* [22]. Identificar e avaliar riscos de cibersegurança orientado pela norma ISO27005 (técnicas de gestão de risco de segurança de informação). O modelo define 6 atividades chave: A1. Categorização de ativos, vulnerabilidades, riscos, entre outros; A2. Identificação de ativos e acessos a estes; A3. Nível de impacto de vulnerabilidade sobre o ativo; A4. Identificação de riscos de cibersegurança sobre os ativos; A5. Medir o risco; A6. Aplicação de contramedidas de segurança. **Relevância**: 5

5. *Ciência organizacional e cibersegurança* [23]. A segurança cibernética como componente de uma ciência organizacional e estudo do fator humano no comportamento organizacional, quer na perspetiva de utilizadores finais, quer na perspetiva de especialistas de cibersegurança, como ameaça (*insider threat*). O estudo utiliza o enquadramento da ISO2700 (Segurança de Informação). O estudo aponta para o benefício da análise preditiva de comportamentos humanos em contexto organizacional, que possam promover incidentes de cibersegurança internos na Organização. **Relevância**: 3

6. *Engenharia Social: Avaliação de Riscos e Vulnerabilidades tendo o Fator Humano como o elo mais fraco da Segurança de Informação* [24]. Estudo de Caso de analise de exploração de vulnerabilidades do fator humano, recorrendo a técnicas de *Social Engineering* (SoE), relativamente à Segurança de Informação de uma Organização. O estudo utiliza o enquadramento das ISO2701 e ISO27002 (Gestão de Sistemas de Segurança de Informação), de uma forma muito generalizada focando-se mais na identificação e analise de tipos de técnicas de SoE. **Relevância**: 2

7. *O papel da conscientização sobre Segurança de Informação dos funcionários sobre a intenção de resistir à engenharia social* [25]. Analise de fatores humanos em contexto organizacional sujeitos a vulnerabilidades de Segurança de Informação por exploração de técnicas de SoE. O estudo analisa uma serie de fatores dos indivíduos inquiridos, tais como conhecimento e formação em Segurança de Informação, intenção, entre outros, mas nenhum dos fatores se foca em fatores psicossociais. No entanto, o estudo conclui que as Organizações não se podem apenas focar em tecnologia como medida para promover a Segurança de Informação, devem assim promover o conhecimento de Segurança de Informação dos seus colaboradores como forma de prevenção a ataques, SoE. **Relevância**: 3

8. *Desenvolvendo um modelo concetual para ameaça interna* [26]. Este artigo correlaciona causas e consequências do foro psicossocial de colaboradores de organizações, na concretização de ciberataques internos a essas organizações. **Relevância**: 5

9. *Relatório Cibersegurança em Portugal - Sociedade 2020* [10]. O Relatório perspetiva uma relação entre os comportamentos individuais e organizacionais com a pandemia Covid-19 e o impacto destes na cibersegurança. **Relevância**: 5

10. *Relatório Cibersegurança em Portugal - Riscos e Conflitos 2021* [27]. O Relatório analisa indicadores do CNCS, do ano de 2020, demonstrando um aumento de atividades ilícitas online, nomeadamente ao nível dos incidentes de cibersegurança e da cibercriminalidade, apontando para a coincidência entre a pandemia Covid-19 e o aumento destes incidentes, relacionando o mesmo com o confinamento social, o trabalho remoto e o uso intenso do digital, durante a pandemia. **Relevância**: 5

As fontes consultadas para a recolha destes contributos, são transversais a várias áreas de domínio: científico, académico, legal, setor empresarial público e de entidades reguladoras no domínio da Segurança de Informação, no entanto a delimitação do tema focou-se no âmbito da gestão de risco e o impacto pandémico da Covid-19, neste domínio. Realça-se assim, que as fontes consultadas, contribuíram para o desenvolvimento da presente dissertação, no sentido em que, vêm relacionar fatores de stress, ansiedade e depressão, com uma maior vulnerabilidade dos colaboradores de organizações a ciberataques, e como essa sintomatologia de doenças do foro psíquico se tornou ainda mais evidentes em período de pandemia e isolamento.

2. Estado de Arte

Os dois modelos mais referenciados nos dias de hoje, no âmbito da presente dissertação, i.e., modelos de gestão de tecnologias de informação, são: o *Information Technology Infrastructure Library* (ITIL) [28] e o *Control Objectives for Information and related Technology* (COBIT) [29]**.** Também relevante é o referencial da *International Organization for Standardization* (ISO) dedicado ao tema Segurança de Informação e Gestão de Risco em Tecnologias de Informação (TI), através da família de standards ISO 27000 e ISO 31000 [30]–[32]. Na Tabela 1 descrevem-se as caraterísticas destes três referenciais, ITIL, COBIT e ISO, no âmbito da Segurança de Informação das Tecnologias de Informação.

Ao nível de governança, i.e., princípios orientadores para a direção de organizações, com modelos de gestão de tecnologias de informação implementados, quer o ITIL, quer o COBIT, ambos têm uma estrutura integrada de modelo de governança, com os restantes processos destes modelos. Já a ISO, também tem o seu modelo de governança espelhado na ISO38500, sendo este, amplo às várias variantes de normas da família ISO no domínio das tecnologias de informação, i.e., não obriga a que seja esse o modelo de governança utilizado num sistema de gestão de tecnologias de informação, podendo optar-se por outro referencial integrado com as restantes normas e processos ISO, no domínio das tecnologias de informação. No entanto, ressalva-se que a presente dissertação, não pretende focar-se nos modelos de governança de sistemas de tecnologias de informação, mas sim, nos processos específicos de Segurança de Informação e Gestão de Risco, de cada um destes referenciais, ITIL, COBIT e ISO.[28], [29], [33]

Tabela 1 – Modelos ITIL, COBIT, e ISO no âmbito da Segurança de Informação no domínio das Tecnologias de Informação [29], [34]–[43]

Modelo	Origem	Orientado para	Versão Atual
ITIL	CCTA Central Compute rand Telecommunications Agency Agência Governamental UK London	Gestão de Serviços TI	ITIL4 2018
COBIT	ISACA Information Systems Audit and Control Association USA	Auditoria e Controlo de Sistemas de Informação e Serviços TI	COBIT 2019
ISO	ISO Internacional Organization for Standardization Vários Membros Europeus	Normalização de várias áreas de domínio científico e Empresarial, entre elas Gestão e Análise de Risco de Segurança de Informação de Serviços TI	20000-1:2018 20000-2:2019 20000-3:2019 27001:2013 27002:2013 27005:2018 27032:2012 31000:2018 31010:2019

No domínio da gestão de serviços e processos TI, o primeiro modelo a ser conhecido, que aborda o âmbito Segurança de Informação como um processo, foi o ITIL. O COBIT também aborda a Segurança de Informação como um processo. As normas da ISO, definiram vários referenciais normativos no domínio da Segurança de Informação em TI, como processos em sistemas de gestão de serviços TI (ISO 27000 e ISO 31000) [30], [31], [44].

2.1. Análise de Modelos

2.1.1. ITIL

O primeiro modelo de referência para gestão de processos e serviços de Tecnologias de Informação, em contexto Organizacional, surge como um modelo com um conjunto de boas práticas de gestão de processos e serviços de tecnologias de informação relacionados com o negócio/âmbito da organização. Integra um processo de gestão Segurança de Informação, dentro da fase do desenho do serviço, conforme se pode verificar na Figura 4 que representa a versão atual do modelo de gestão de TI do ITIL.

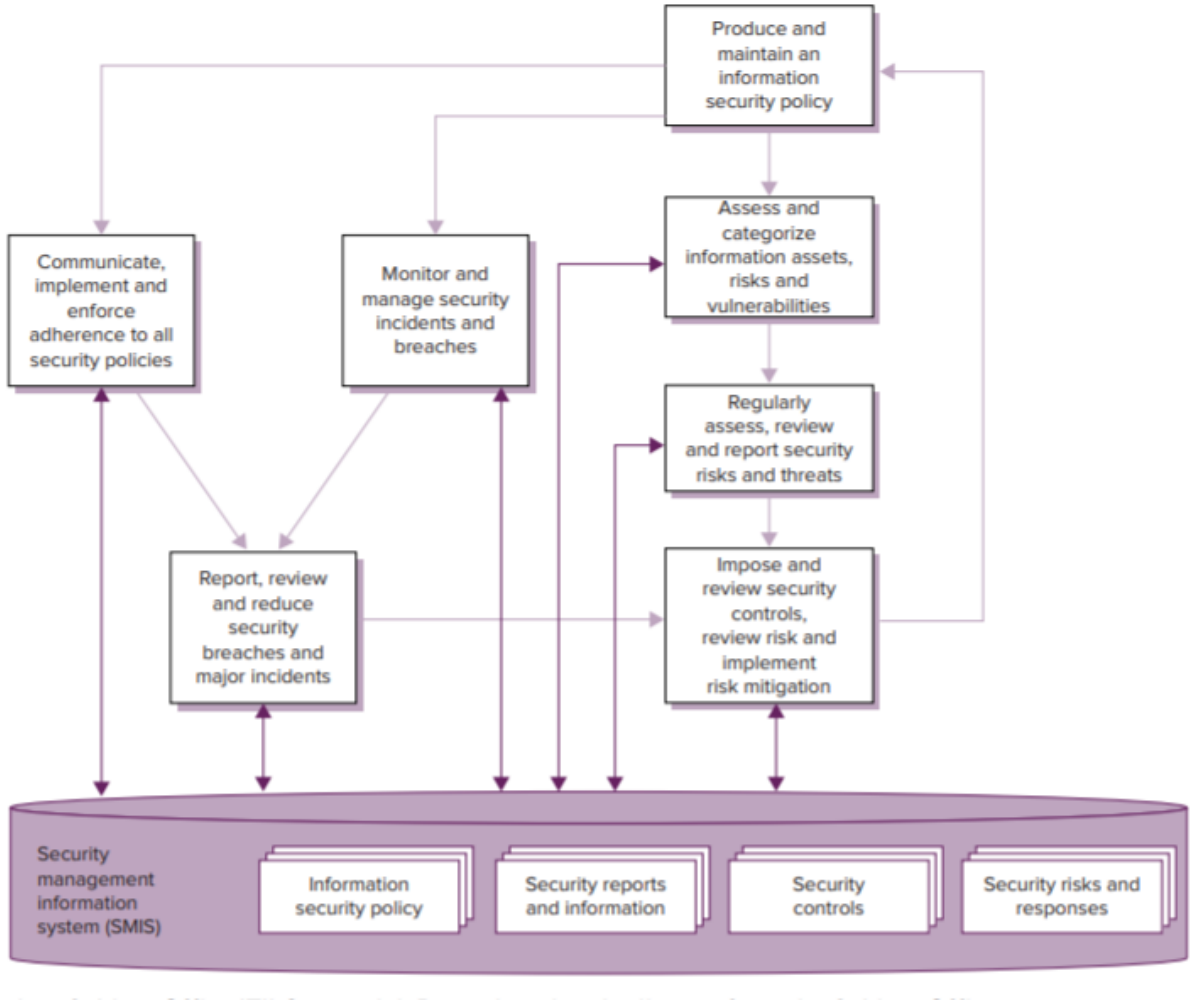

Figura 4 – Processo de Gestão de Segurança de Informação e Fase de Gestão de Risco ITIL **Fonte**: [28]

Na Figura 4 observa-se que, o **ITIL**, apresenta a possibilidade de implementação de um Sistema de Gestão de Segurança de Informação (SGSI), onde se incluem várias atividades desde a definição de uma politica de segurança, a identificação de ativos e vulnerabilidades e ameaças a que estão sujeitos, análise de risco sobre os ativos e aplicação de controlos de segurança e monitorização de todo o sistema de gestão de Segurança de Informação. Todas estas atividades contribuem de forma relacionada para os processos do SGSI, nomeadamente Política de Segurança de Informação, Relatórios de Segurança de Informação, Controlos de Segurança e Resposta a Riscos de Segurança.

A visão da Segurança de Informação no ITIL, é um processo orientado para a Segurança de Informação tratada do domínio do negócio da organização, é um processo independente dos restantes processos do ITIL, como por exemplo processo de continuidade, processo de alterações, entre outros. Evidencia-se assim, o facto do processo de Segurança de Informação não ser amplo a todos os restantes processos do ITIL e assim sendo, a análise de gestão de risco de Segurança de Informação no ITIL não tem uma visão da Segurança de Informação em todos os processos, mas apenas orientada, especificamente, para a informação tratada dentro do negócio. Cada processo no ITIL, tem a sua fase de análise e gestão de risco, não existe uma visão de um processo único de gestão de risco amplo a

todos os processos do ITIL com uma visão holística dos efeitos e contributos de todos os processos e da importância do processo de Segurança de Informação sobre todos esses processos.

Por outro lado, conforme observado na Figura 5, o facto do processo de gestão de Segurança de Informação estar definido, na fase do ciclo de vida do serviço **ITIL**, "*Service Design*", ao invés de ser definido na fase de estratégia "*Service Strategy"*, faz com que o seu valor não seja refletido de modo elevado, ao nível da estratégia da organização, ou seja, a estratégia continua a ser orientada para o negócio e serviços da organização, o que, numa visão geral de um modelo de gestão de risco de Segurança de Informação coloca este conceito fora de decisões estratégicas da organização ou pelo menos, coloca o mesmo num nível de importância inferior ao do negócio para a organização. Quando nos dias de hoje, a informação é o ativo mais importante para a organização e para o seu negócio.

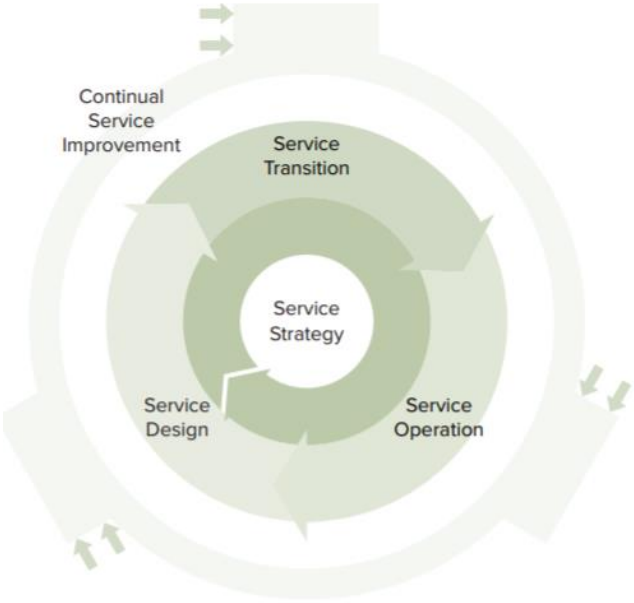

Figura 5 – Ciclo de Vida Serviço ITIL **Fonte**: [28]

Por cada serviço TI numa organização, o modelo **ITIL** define um processo de gestão de Segurança de Informação, bem como um subprocesso de gestão de risco inerente, na fase de desenho do serviço, ao invés de definir um processo de gestão na fase estratégica do serviço e amplo a todo o ciclo de vida do serviço.

Em suma, o **ITIL** está orientado para o negócio da organização e não, especificamente, para a Segurança de Informação dos seus serviços TI, assim sendo, também a aplicabilidade de um modelo de gestão de risco de Segurança de Informação, neste modelo, não terá uma amplitude estratégica para este âmbito.

2.1.2. COBIT

O modelo **COBIT** foi criado pela associação americana *Information Systems Audit and Control Association* (ISACA) [29]. Este modelo está essencialmente focado na auditoria e otimização de recursos TI numa organização, de acordo com os objetivos de negócio definidos, isto significa que não

é apenas focado nos serviços e processos TI, mas sim, na adaptação destes ao negócio da organização. O COBIT disponibiliza assim, um conjunto de boas práticas, para aplicação de controlos que otimizem os investimentos nas tecnologias de informação de determinada organização.

Na Figura 6, podemos observar que o modelo **COBIT** é constituído por 37 processos, 32 dedicados à gestão e 5 dedicados à liderança. Dentro dessas duas vertentes, o COBIT identifica ainda 5 domínios de ação: Avaliar, Gerir e Monitorizar; Alinhar, Planear e Organizar; Construir, Adquirir e Implementar; Entrega, Serviço e Suporte; Monitorizar, Avaliar e Aferir. Dos 32 processos dedicados à gestão, um pertence à Segurança de Informação e outro à Gestão do Risco, ambos alinhados com as atividades do modelo COBIT designadas por Alinhar, Planear e Organizar. Nesta versão, o COBIT, tem um processo dedicado à Segurança de Informação com o objetivo conjunto de procurar proteger os princípios integridade, confidencialidade e disponibilidade da informação, alinhado com os objetivos de negócio da organização. Na realidade o COBIT, na sua última versão faz uma abordagem a uma integração de vários referenciais de boas práticas, normas e modelos, associadas ao domínio da Segurança de Informação, com a intenção de tirar o melhor proveito e compreensão, de como cada uma delas se relaciona com o domínio da Segurança de Informação integrada em contexto organizacional.

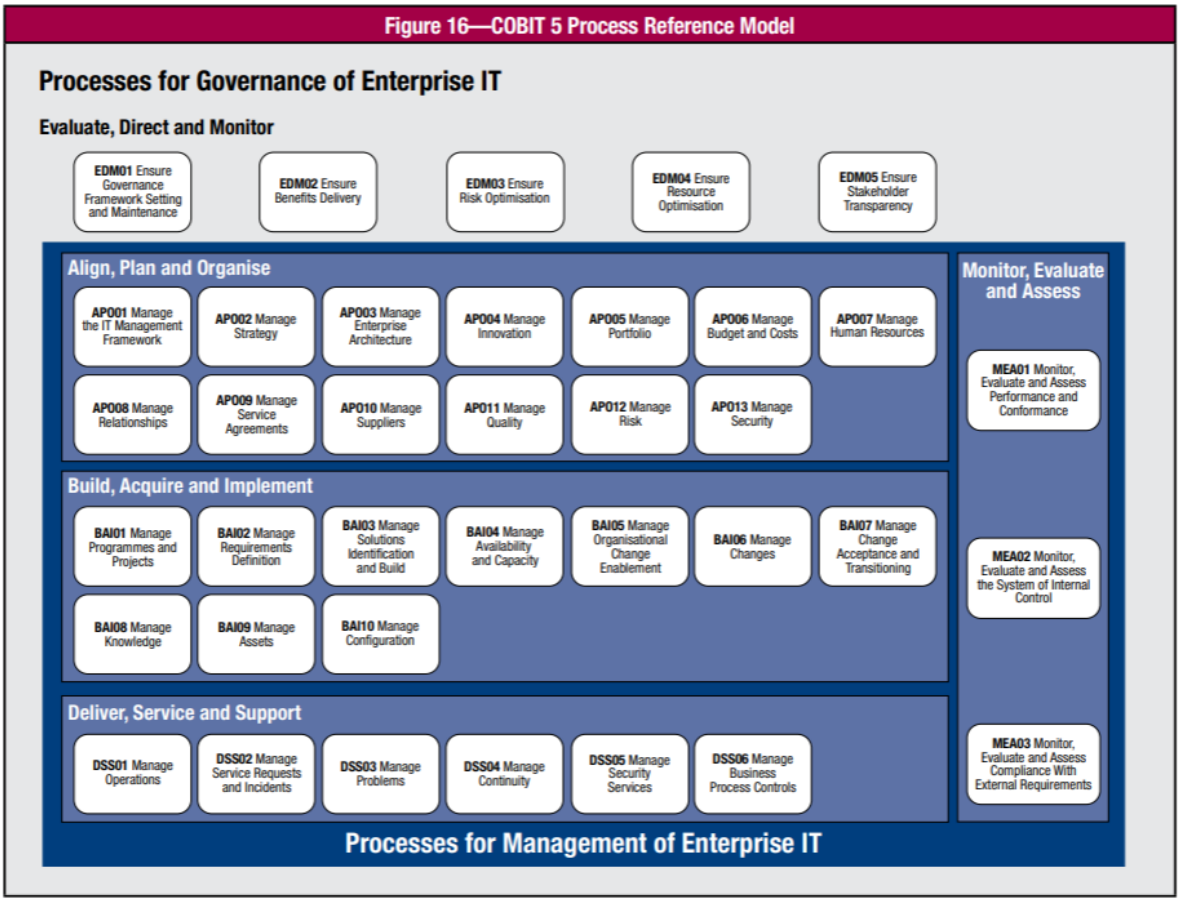

Figura 6 – Processos e Atividades Modelo COBIT 5 **Fonte**: [29]

No âmbito da gestão do risco aplicada à Segurança de Informação, o COBIT, faz uma abordagem à defesa do negócio, em função da proteção da informação confidencial tratada nas aplicações de negócio críticas. Nesta vertente de gestão do risco, o COBIT baseia-se nos princípios: suporte ao negócio, defender o negócio e promover um comportamento responsável de Segurança de Informação.

Em suma, o modelo COBIT, define um conjunto de processos, em que cada processo é constituído por um conjunto de atividades, que permitem medir o desempenho dos objetivos do processo definidos de acordo com o negócio da organização, é portanto, um modelo orientado para o negócio de determinada organização, onde a gestão de Segurança de Informação e a gestão do risco são processos de gestão no domínio Alinhar, Planear e Organizar, ou seja, não está focado na execução destes dois processos mas sim no seu alinhamento com o negócio da organização.

2.1.3. Normas de Segurança ISO

Inclui várias normas orientadas para serviços TI, tais como: Gestão de Segurança de Informação, Gestão de Serviços de Tecnologias de Informação, Gestão de Risco, entre outros. Ao contrário das restantes referências e modelos, as normas **ISO** definem processos de gestão de serviços TI focados na Segurança de Informação, com um processo de gestão de risco especificamente orientado para esse fim. Neste modelo, a Segurança de Informação passa a assumir o papel fulcral levando em consideração o negócio da empresa, mas não agindo unicamente em função do mesmo e dos serviços que o definem, ao contrário do ITIL e do COBIT.

De modo a efetuar uma analogia direta entre a ISO, ITIL e COBIT, o modelo mais semelhante será o da ISO 20000-1:2018 (primeira versão em 2005), demonstrado na Figura 7, onde podemos observar um sistema de gestão de serviços TI orientado para processos dentro de um âmbito Organizacional, em que se pode observar um processo de gestão de Segurança de Informação na camada operacional do sistema de gestão. Este sistema de gestão não é composto por hierarquias ou estrutura sequencial de processos e serviços, mas sim de um conjunto de relações entre eles, dentro do âmbito do sistema de gestão definido. Também se destaca o facto da definição de Segurança de Informação do sistema, dar-se a um nível estratégico, na definição de políticas pela decisão superior (decisão de gestão estratégica da organização). Já a fase de análise e gestão de risco é inserida na camada de planeamento do sistema de gestão, abrangendo todo o sistema de gestão.

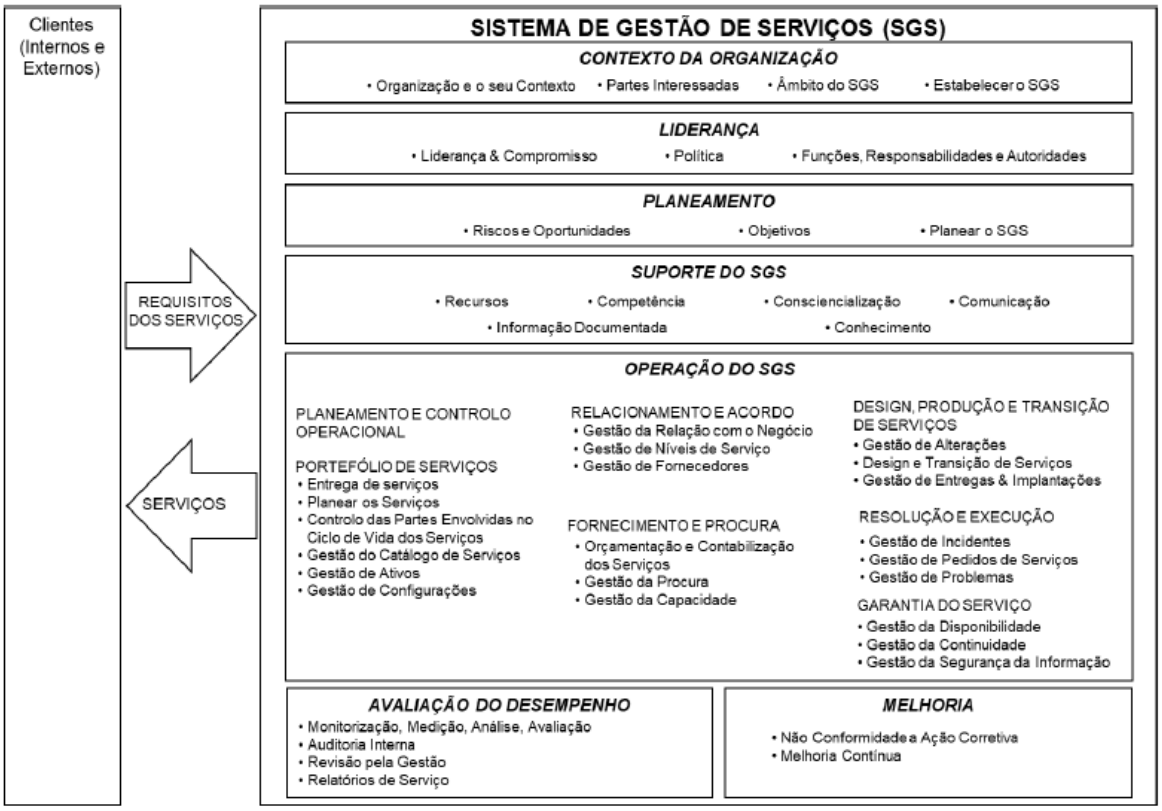

Figura 7 – Processos e Serviços Modelo ISO 20000-1:2018 **Fonte**: [36]

Já a fase de análise e gestão de risco, é inserida na camada de planeamento do sistema de gestão, abrangendo todo o sistema de gestão, com a referência ao modelo da ISO31000:2018, do qual fazem parte as fases demonstradas na Figura 8.

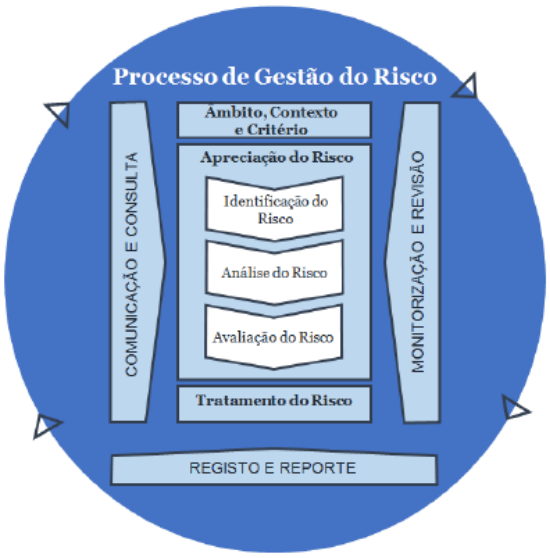

Figura 8 – Processo Gestão de Risco ISO 31000.2018 **Fonte**: [35]

É verificado que, quer o processo de Segurança de Informação, quer o processo de análise e gestão de risco, são orientados ao sistema de gestão e estratégia definida a todo o contexto da organização.

Pese embora a ISO tenha implementado a norma ISO20000-1:2018, conjugada com a ISO31000:2018, especificamente para implementação de sistemas de gestão de serviços TI, com a definição de processos de gestão de Segurança de Informação e gestão de risco, o sistema de normalização ISO implementou vertentes especificas para a temática Segurança de Informação e Gestão de Risco neste contexto, ou seja, para a implementação de um Sistema de Gestão de Segurança de Informação (SGSI), entre elas a ISO27001:2013 e a ISO27005:2018.

Para a construção do modelo de gestão de risco, em resposta ao objetivo definido na presente dissertação, foram utilizados os referenciais normativos: ISO31000:2018, ISO31010:2019, ISO27001:2013, ISO27002:2013, ISO20000-1:2018, ISO20000-2:2019, ISO20000-3:2019, ISO27005:2018 e ISO27032:2012, tendo em vista a conceção de um modelo de gestão de risco aplicado à Segurança de Informação da ANSR, com foco nas possíveis ameaças via Engenharia Social. A principal razão para a escolha destes referenciais é o facto de ser possível analisar especificamente as ameaças e vulnerabilidades retratadas na presente dissertação, ou seja, ameaças de insider threats e vulnerabilidades de trabalho não supervisionado (anexos C e D da ISO27005). Na Tabela 2 demonstra-se o conteúdo de cada um destes referenciais, utilizado para resposta ao objetivo da dissertação [35]–[43].

Tabela 2 – Conteúdos integrados ISO para *Modelo de Gestão de Risco* proposto [45]

NORMA	ÂMBITO	CONTEÚDO INTEGRADO PARA O MODELO DE GESTÃO DE RISCO DE SEGURANÇA DE INFORMAÇÃO [5 a 13]
ISO31000:2018	Metodologia do processo de gestão de risco, aplica conceitos especificados na norma ISO31010:2019.	Orientações: Especificação das fases do processo de gestão de risco Figura 8
ISO31010:2019	Orientação sobre a seleção e aplicação de técnicas para avaliação de risco em uma ampla gama de situações, com referência a outros documentos onde as técnicas são descritas com mais detalhes, aplica conceitos especificados na norma ISO31000:2018.	Orientações: . Conceitos no domínio da gestão de risco; . Anexo A Características e técnicas de análise e gestão de risco.
ISO27001:2013	Requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de Segurança de Informação no contexto da organização, abordagem requisitos para a avaliação e tratamento dos riscos de Segurança de Informação ajustados às necessidades da organização, aplica conceitos especificados nas normas ISO27002:2013, ISO27005:2018 e ISO31000:2018.	Orientações: . Anexo A Controlos de Segurança de Informação aplicados para modificação do risco (Ativos, Classificação da Informação, teletrabalho, organização, entre outros).
ISO27002:2013	Diretrizes para a seleção, implementação e gestão de controlos de Segurança de Informação num Sistema de Gestão de Segurança de Informação baseado na ISO27001:2013. Aplica conceitos especificados nas normas ISO20000-1:2019, ISO20000-2:2019, ISO27001:2013, ISO27005:2018 e ISO31000:2018.	Orientações: . Descrição e detalhe dos controlos de Segurança de Informação aplicados para modificação do risco pela ISO27001:2013.

NORMA	ÂMBITO	CONTEÚDO INTEGRADO PARA O MODELO DE GESTÃO DE RISCO DE SEGURANÇA DE INFORMAÇÃO [5 a 13]
ISO27005:2018	Gestão de riscos de Segurança de Informação, aplica os conceitos especificados nas normas ISO27001:2013, ISO27002:2013 e ISO31000:2018, de modo a implementar a Segurança de Informação com base numa abordagem de análise de risco de Segurança de Informação da organização.	Orientações: . Anexo A âmbito do modelo de gestão de risco; . Anexo B identificação dos ativos e avaliação de impacto dos mesmos; . Anexo C identificação de ameaças especificas e origens; . Anexo D identificação de vulnerabilidades; . Anexo E abordagem na análise de risco e valorizações ativos vs vulnerabilidades vs ameaças; . Anexo F controlos aplicados para modificação do risco.
ISO27032:2012	Orientação para abordar problemas de Cibersegurança, com destaque para as características desta atividade e relação com outros domínios como por exemplo a Segurança de Informação e gestão de risco, aplica os conceitos das normas ISO27001:2013, ISO27005:2018 e ISO31000:2018.	Orientações: . Conceitos no domínio da Cibersegurança; . Controlos de Cibersegurança específicos para ataques Engenharia Social.
ISO20000-1:2018	Requisitos para implementação de um sistema de gestão de serviços TI, aplica os conceitos das normas ISO27001:2013, ISO20000-2:2019, ISO20000-3:2019 e ISO31000:2018.	Orientações: . Processo de Gestão de Segurança de Informação.
ISO20000-2:2019	Recomendações para implementação de um sistema de gestão baseado na ISO20000-1:2018. Aplica os conceitos das normas ISO27001:2013, ISO20000-1:2018, ISO20000-3:2019 e ISO31000:2018.	Orientações: . Descrição e detalhe dos requisitos para implementação de um sistema de gestão baseado na ISO20000-1:2018.
ISO20000-3:2019	Recomendações sobre a definição do âmbito e aplicabilidade do mesmo aos requisitos especificados na ISO20000-1:2018 face à organização. Aplica os conceitos das normas ISO27001:2013, ISO20000-1:2018 e ISO20000-2:2019.	Orientações: . Descrição e detalhe dos requisitos para implementação de um sistema de gestão baseado na ISO20000-1:2018.

Isto significa que, ao contrário do ITIL e COBIT, a ISO permite a implementação de um SGSI, específico e orientado unicamente para a Segurança de Informação e Gestão de Risco desta, i.e., permite às organizações implementarem um SGSI orientado para a Segurança de Informação num determinado contexto organizacional e não para os serviços desta. Nesta realidade, as organizações podem optar pela implementação de sistemas de gestão unicamente focados na Segurança de Informação e devida análise de risco, sem a ligação direta ou obrigação de implementarem também um Sistema de Gestão de Serviços TI (SGSTI).

As normas ISO permitem também, implementar sistemas integrados, ou seja, um Sistema de Gestão de Segurança de Informação Integrado com um Sistema de Gestão de Serviços TI, podendo inclusive ser implementado um sistema integrado entre uma ISO27001:2013, ISO27005:2018, com a ISO20000-1:2018, ou com ITIL ou COBIT. Existem normas da ISO que permitem este tipo de implementações, ou seja, implementar uma realidade de gestão de Segurança de Informação e análise de risco desta pela ISO, conjugada com um sistema de gestão de serviços TI pelas normas ITIL ou COBIT.

Em suma, as ISO possibilitam um foco único para a temática Segurança de Informação e gestão de risco implícita, contrariamente aos seus pares, ITIL e COBIT, que têm uma implementação única de um sistema de gestão orientado para serviços TI do qual faz parte a Segurança de Informação e a análise de risco do sistema de gestão implementado. Os modelos ITIL e COBIT são, na sua essência, orientados para modelos de gestão empresarial anglo-saxónicos, cujo fio condutor da decisão são os acionistas e assim sendo é o negócio. Já as normas ISO, permitem que a estratégia do mesmo seja em torno da Segurança de Informação e não, unicamente, no negócio da empresa [46].

Na Figura 9 pode ser observado o crescimento de adesão de empresas portuguesas à normalização ISO, especificamente à ISO27001 Sistema de Gestão de Segurança de Informação e base de implementação da ISO27005 Gestão de Risco da Segurança de Informação. Por outro lado, no que respeita à ISO 20000-1 Sistema de Gestão de Tecnologias de Informação, existe um decréscimo de empresas aderentes. Esta diferença de crescimento de adesão, entre as ISO27001 e a ISO20000-1, resulta do facto da maior parte das empresas passarem a focar-se unicamente numa perspetiva de Sistema de Gestão orientado à Segurança de Informação (ISO27001), ao invés de implementarem Sistemas de Gestão de Serviços de Tecnologias de Informação onde a Segurança de Informação é um apenas um processo e não o foco estratégico (ISO20000-1). Ainda assim, e de uma perspetiva preocupante, no domínio da Segurança de Informação, esta temática. ocupa um nível de investimento por parte das empresas portuguesas, muito baixo, comparativamente com outras áreas certificadas, como por exemplo qualidade, ambiente, entre outras [47].

Nº Certificados	Sist.Gestão	2016	2017	2018	2019
ISO 9001	Qualidade	5589	5837	5743	5827
ISO 14001	Ambiente	1123	1174	1174	1202
SST (45001&18001&4	SST	561	734	674	645
ISO 22000	Seg.Alimentar	295	298	296	294
ISO 50001	Energia	0	27	31	30
ISO/IEC 27001	T.Informação	35	46	63	87
ISO/IEC 20000-1	S.Informação	0	10	11	6
NP 4457	ID&Inovação	170	164	161	157
NP 4406	Florestal	12	14	16	14
NP 4512	Formação Prof.	1	1	1	0
NP 4552	Conciliação	0	0	0	7
TOTAL		7786	8305	8170	8262

BDEC - Base de Dados de Empresas Certificadas

certificação acreditada

IPAC

Versão 1 (31 de março de 2020) - Dados de 2019

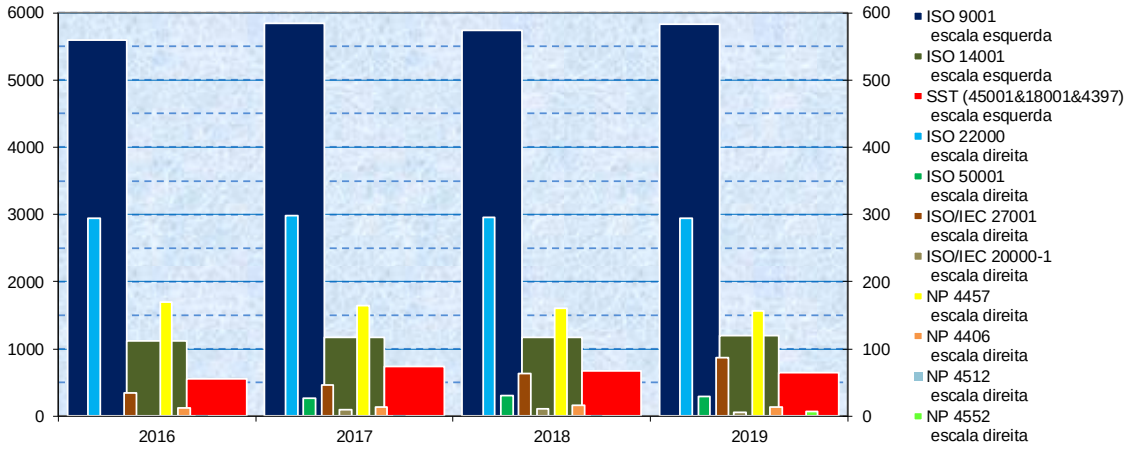

Figura 9 – Evolução da ISO até 2019 **Fonte**: IPAC, "BASE DE DADOS NACIONAL SISTEMAS DE GESTÃO CERTIFICADOS," 2020 [47]

2.2. Comparação ITIL, COBIT e ISO

Os modelos apresentados surgiram em anos diferentes e em contextos distintos, o ITIL e COBIT foram inicialmente apresentados e desenvolvidos à medida das estruturas organizacionais dos seus países de origem, enquanto que a ISO teve desde a sua origem um impulso a nível mundial. Destes três modelos a ISO foi a primeira a abordar o contexto gestão de Segurança de Informação e processo de gestão de risco dedicado a este domínio. É também a ISO o modelo com a revisão mais recente quer pela 27001 quer pelas restantes normas que a apoiam e que já referenciamos no ponto anterior.

Por outro lado, tanto o ITIL como o COBIT nas suas últimas versões, em que abordam a temática Segurança de Informação, referenciam estar alinhados com a ISO27001 e ISO20000. No entanto a referência destes modelos não é feita à versão mais recente da ISO27001, o que os torna desatualizados relativamente a este padrão, verificando que a referência feita por ambos é à versão de 2005 e a última versão da ISO27001 data de 2013.

De um modo conclusivo, a ISO tem o seu foco na gestão da Segurança de Informação, já o ITIL é essencialmente orientado para a gestão de serviços TI, onde apresenta um processo de gestão de Segurança de Informação que tenta abranger as várias fases do ciclo de vida de um serviço, com um foco principal na fase de Desenho do Serviço, por outro lado o COBIT apresenta o seu foco principal na gestão e liderança de TI. Destes três modelos, apenas a ISO tem uma vertente de certificação. Na

Figura 10 destacam-se as vantagens e desvantagens apuradas nos modelos ISO, COBIT e ITIL, como resumo de todos os pontos abordados no Estado de Arte.

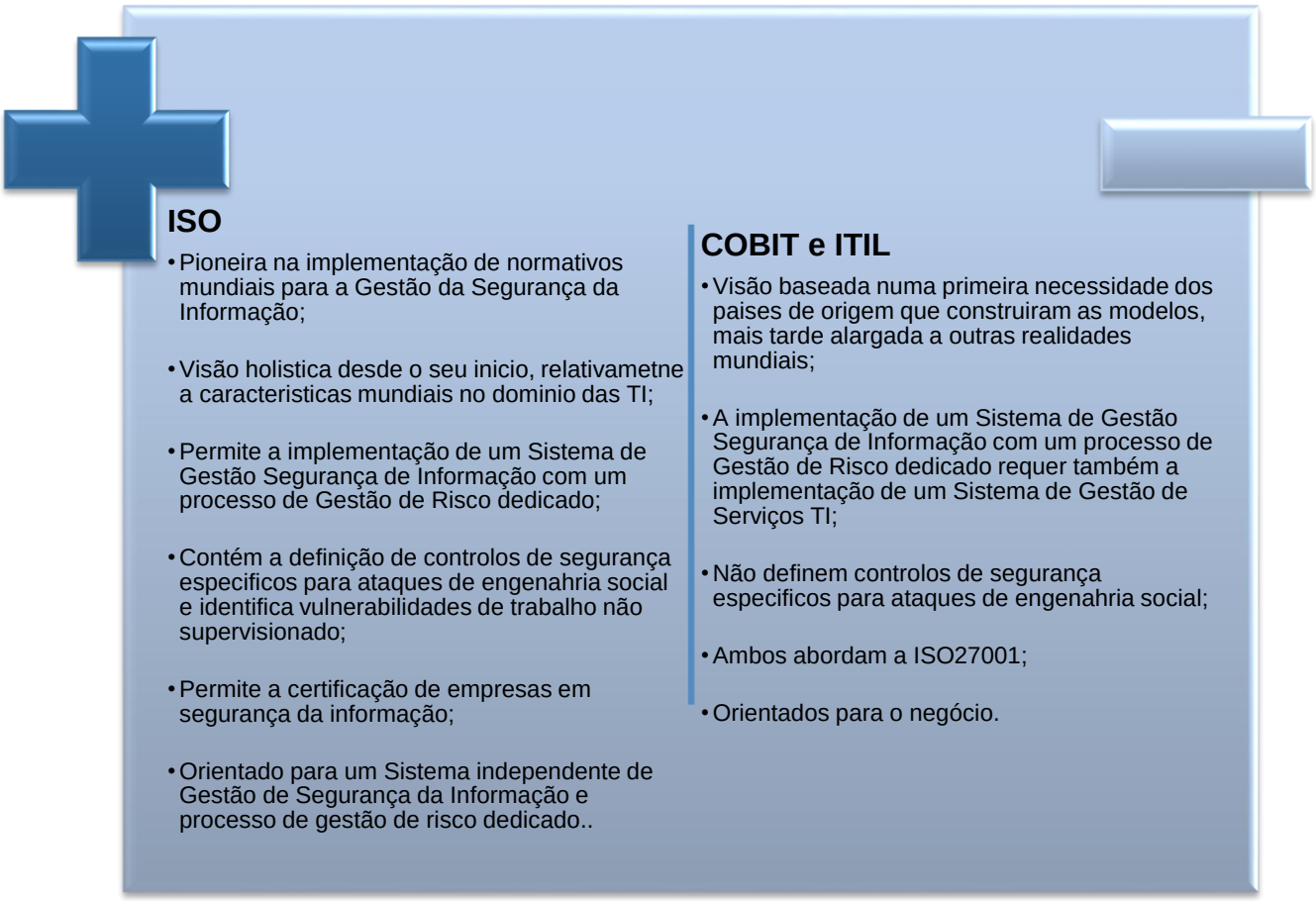

Figura 10 – Vantagens ISSO face ao COBIT e ITIL

3. Modelo Selecionado para Gestão de Risco Intrínseco de Ativos

Respondendo claramente à **questão 1)** do ponto 4. do capítulo I "Qual o modelo adequado para avaliar e monitorizar o risco para a Segurança de Informação?". Face ao contexto do Estado de Arte, bem como à Análise de Modelos abordados no presente capítulo II, o modelo adequado para avaliar e monitorizar o risco para a Segurança de Informação é o modelo ISO, que se descreve infra.

No que concerne a Segurança de Informação e Gestão de Risco implícita, os referenciais ISO 31000 e ISO 27005, com os contributos dos restantes normativos ISO associados à Gestão de Segurança de Informação e Gestão de Serviços TI, são os mais específicos nesta matéria, e por este motivo será a metodologia escolhida para o modelo de gestão de risco a aplicar no Caso de Estudo retratado na presente dissertação.

A utilização do modelo **ISO** permite a conjugação de várias normas, no sentido de se implementar um sistema de gestão de Segurança de Informação, onde um dos processos implícitos é o processo de gestão de risco de Segurança de Informação. Vamos assim, definir um modelo de gestão de risco, com a aplicabilidade das ISO31000 e ISO27005 e contributos das ISO31010, ISO27001, ISO27002, ISO27032, ISO20000-1, ISO20000-2 e ISO20000-3, de acordo com conteúdos indicados na Tabela 2, obtendo a visão do modelo demonstrado na Figura 11, onde todas estas normas se relacionam entre si para o modelo definido.

Figura 11 – Contributos ISO para a construção do modelo de gestão de risco

Os contributos normativos demonstrados na Figura 11 são aplicados nas várias fases do processo de implementação do modelo de gestão de risco. Pela conjugação da ISO31000 e ISO27005, obtemos as fases do processo de implementação do modelo de gestão de risco demonstrado na Figura 12, assim, para cada uma das fases apresentadas contribuem definições e orientações das ISO31010, ISO27001, ISO27002, ISO27032, ISO20000-1, ISO20000-2 e ISO20000-3, de acordo com conteúdos indicados na Tabela 2. Será este o modelo a implementar, em que, os ***inputs*** do mesmo serão apurados na fase Apreciação do Risco - *Risk Assessment*-" com a identificação de ativos, vulnerabilidades e ameaças afetas a esses, no Âmbito -*Context Establishment*- do cenário abordado no Caso de Estudo, e os ***outputs*** serão a quantificação do nível de risco intrínseco também nessa fase.

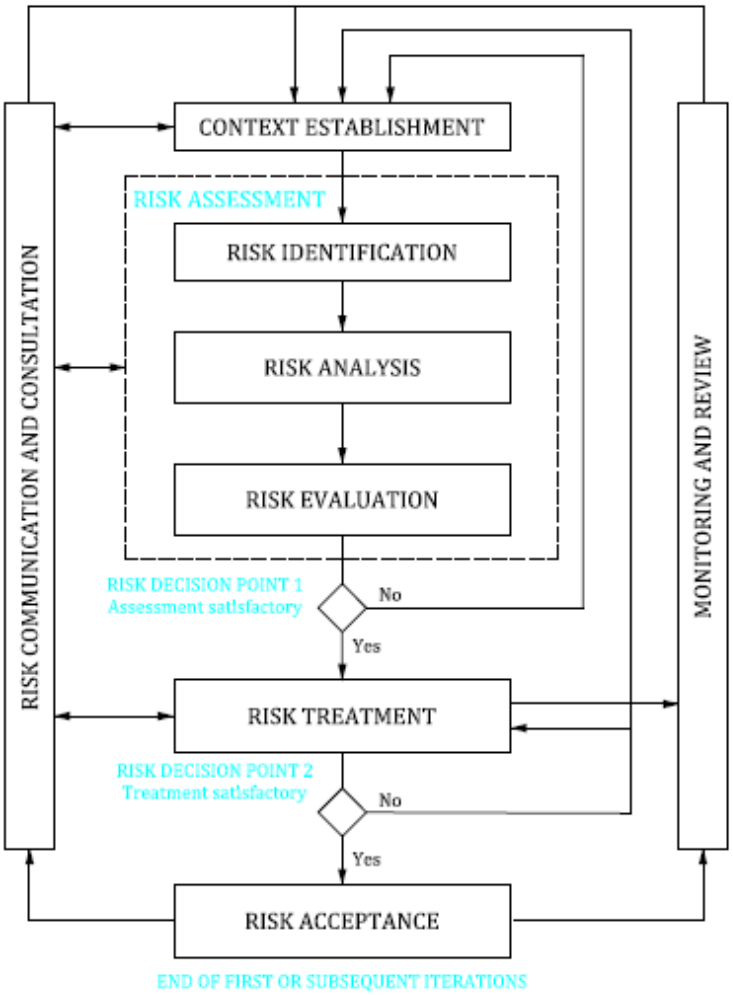

Figura 12 – Processo para implementação de Modelo de Gestão de Risco de Segurança de Informação ISO31000:2018 conjugada com a ISO27005:2018 Fonte: ISO31000:2018 conjugada com a ISO27005:2018 [40]

Pese embora tenham sido analisados outros modelos de gestão de risco, aplicados a Segurança de Informação em matéria de tecnologias de informação, tais como ITIL e COBIT, facto é que nenhum destes, tem um foco e orientações especificas para um modelo de gestão de risco orientado a ameaças de *insider threats* e vulnerabilidades de trabalho não supervisionado, com a indicação e recomendação de controlos específicos de segurança para essas duas circunstâncias, ao contrário do referencial ISO27005, que integrado com as restantes ISO identificadas na Tabela 2 respondem exatamente à aplicabilidade de um modelo de gestão de risco de Segurança de Informação de modo a assegurarem o objetivo da presente dissertação. Para além deste facto, ao contrário do ITIL e COBIT, a ISO permite que as organizações obtenham um selo de certificação em Segurança de Informação, que assegura um grau de confiança neste domínio perante os seus *stakeholders*. Acresce ainda constatar, que a maioria dos artigos científicos, referenciados na Revisão da Literatura, quando se referem a Segurança de Informação evocam maioritariamente a *standard* ISO.

CAPÍTULO III - Metodologia Proposta para Avaliação do Risco e Segurança

1. Metodologia

Conforme referido no ponto 3, do Capitulo II, o modelo aplicado no presente caso de estudo, baseia-se nas fases especificas Âmbito -*Context Establishment*- e Apreciação do Risco - *Risk Assessment*-, especificamente retratadas na Figura 13. De um modo geral, no presente Capítulo, demonstra-se a aplicabilidade deste modelo às organizações.

Figura 13 – Âmbito –Context Establishment- e Apreciação do Risco –Risk Assessment- do Processo para a implementação de Modelo de Gestão de Risco de Segurança de Informação Fonte: ISO31000:2018 conjugada com a ISO27005:2018 [40]

2. Âmbito - Context Establishment

A definição do âmbito de aplicação do modelo de gestão de risco, e sobre o qual irá recair a fase de apreciação o risco, resulta da identificação correta de todas as componentes da organização, que produzem, acedem, tratam e disponibilizam informação, no sentido de identificar onde, como e com que probabilidade se podem concretizar riscos numa Organização. Por componentes podem ser entendidas dimensões tais como: recursos humanos (internos e externos), fornecedores, clientes, sistemas de informação, documentação classificada, infraestrutura tecnológica, dispositivos de hardware, legislação, entre outros. O âmbito de aplicação do modelo de gestão de risco, de uma organização, numa perspetiva de **Segurança de Informação**, está diretamente associado a todas as formas, suportes e canais de circulação, da informação dessa organização. [2]

Podemos assim, aplicar o Anexo A da ISO27005 (A.1), para a definição do âmbito a adotar, onde são tidos em conta fatores da organização tais como: A Identidade da organização; os seus Objetivos Estratégicos; Missão e Valores e a Estrutura da organização.[40]

3. Apreciação do Risco - Risk Assessment

A fase de Apreciação do Risco, pressupõe a aplicação de três processos específicos: Identificação do Risco, Analise do Risco e Avaliação do Risco. Assim, dentro do âmbito definido, importa entender os processos:

3.1. Identificação do Risco

Este processo, consiste em identificar os ativos a proteger e possíveis relações entre si, mais uma vez, tendo em conta o âmbito definido. Neste processo, é efetuado um **inventário de ativos** da organização, em que um ativo é um item que suporta informação com valor para a Organização. [2]

Pela aplicação do Anexo B da ISO27005 (B.1), para a apreciação do risco evidencia-se a necessidade de identificar os ativos do âmbito definido, existindo claramente uma distinção entre ativos primários e ativos secundários de suporte, em que [40]:

Ativos Primários – Definem-se como os processos de negócio e a informação classificada neles gerada. Assim, no Caso de Estudo retratado na presente dissertação, o ativo primário será o Processo de Contraordenação Rodoviária da ANSR, demonstrado na Figura 14, do n.º 1, do Capitulo IV, que contribui para o Planeamento e Coordenação a nível nacional de apoio à política do Governo em matéria de segurança rodoviária e a aplicação do direito contraordenacional rodoviário, bem como a Informação Classificada gerada.

Ativos Secundários - Ativos de suporte aos ativos primários, tais como hardware, software, rede, pessoal, site e estrutura organizacional.

Conforme referenciado no Anexo B da ISO27005 (B.1.2), dependendo da finalidade do estudo a efetuar, poder-se-á dar o caso de não ser necessária uma análise exaustiva de todos os elementos que compõem o âmbito do mesmo, nestes casos podem ser limitados os ativos a identificar aos elementos-chave desse âmbito. Assim, no caso aqui retratado delimitamos os ativos identificados ao âmbito do ponto 2. do presente Capítulo e ilustrado na Figura 22. em que [40]:

Ativo Primário

- Processo Administrativo Interno da ANSR que contribui para o Planeamento e Coordenação a nível nacional de apoio à política do Governo em matéria de segurança rodoviária e a aplicação do direito contraordenacional rodoviário, bem como, a Informação classificada nele gerada.

Ativo Secundário

- Equipamentos portáteis utilizados pelos colaboradores em regime de teletrabalho da ANSR no âmbito das suas funções profissionais e que contribuem para o Ativo Primário identificado.

A primeira fase de apreciação do risco (*Risk Assessement*) resulta da identificação dos ativos secundários no anexo B da ISO27005 (B.1.3), do âmbito, que possam ter vulnerabilidades e que podem ser exploradas por ameaças que visam prejudicar os ativos primários do âmbito (processos e informação) [40].

A segunda fase, passa por elaborar o inventário de Ativos, que deve permitir valorizá-los em função do seu impacto para a Organização, para este efeito define-se uma **matriz de impacto**, com Níveis de Impacto e Linhas Orientadoras para a análise de impacto, de modo a quantificar o ativo, face á concretização de uma ameaça, numa perspetiva de ausência de controlos de Segurança de Informação sobre os ativos avaliados. [2]

Pela aplicação do Anexo B da ISO27005 (B.2), podemos definir uma matriz de impacto para valorização dos ativos identificados, com as linhas orientadoras para a análise desse impacto, de modo a quantificar o mesmo caso exista concretização de uma ameaça. Pese embora a lista de particularidades identificadas no Anexo A da ISO27005 (A.2 e A.3), tais como questões de natureza politica, territoriais, climáticas, económicas, etc…esta referência não é delimitadora na abordagem a adotar. [40]

3.2. Análise do Risco

Este processo, consiste em **identificar as ameaças** às quais, se considera, que possam estar expostos os ativos por exemplo.: desastres naturais (sismos, terramotos, etc), manipulação de informação e cópias de informação, corrupção, abuso de direitos de perfil de administração de rede informática, acesso físico ou logico não autorizado, etc… Para além deste pressuposto, é também necessário **identificar as vulnerabilidades** a que estão expostos os ativos, ou seja, condições dos ativos que possam favorecer a concretização de determinada ameaça e até mesmo o impacto da mesma. [2]

Para a identificação de ameaças, e no contexto da presente dissertação, iremos focar-nos nas ameaças com recurso a engenharia social, descritas no Anexo C da ISO27005, assim, identificadas as **ameaças**, será ainda necessário definir os níveis de cada uma delas, **Baixa**, **Média** ou **Alta**, dependendo do numero de vezes que as mesmas se concretizaram em determinado período. Para a identificação das **vulnerabilidades** de acordo com as recomendações do Anexo D da ISO27005, identifica-se a principal vulnerabilidade o facto dos ativos estarem em teletrabalho sem supervisão do seu trabalho por perfis de responsabilidade da organização, sendo também necessário definir os níveis de concretização de cada uma delas, **Baixa**, **Média** ou **Alta**, dependendo da probabilidade de concretização dessa vulnerabilidade em determinado período [40].

3.3. Avaliação do Risco

Este processo, consiste em **calcular o risco intrínseco dos ativos**, ou seja, apurar o risco de Segurança de Informação a que os ativos estão sujeitos, aquando do momento em que os mesmos se encontrem sem qualquer aplicação de medidas de segurança, em função das ameaças e vulnerabilidades que lhes são aplicáveis. [2]

Para esta fase, pode ser definida uma matriz, tendo em conta a metodologia utilizada no Anexo E ISO27005, onde para cada Classe de Ativos, face ao seu valor de ameaça e ao seu valor de vulnerabilidade, irá originar um determinado de valor de Risco Intrínseco de cada ativo [40].

3.4. Definição do Risco Aceitável

A **definição do risco aceitável**, depende da estratégia e decisão de topo da organização, ou seja, depende da decisão de qual o limite de risco, a partir do qual, se entende ser necessário aplicar um procedimento de tratamento do risco sobre determinado ativo, cujo valor de risco intrínseco é superior ao risco aceitável definido pela organização. [2]

CAPÍTULO IV - Caso de Estudo: Descrição dos Processos Objeto de Avaliação do Risco e Segurança

1. Caracterização do Caso de Estudo

A Autoridade Nacional de Segurança Rodoviária (ANSR) é um serviço central da administração direta do Estado dotado de autonomia administrativa, que tem por missão o planeamento e coordenação a nível nacional, de apoio à política do Governo em matéria de segurança rodoviária, bem como, a aplicação do direito contraordenacional rodoviário [48]. A ANSR, tem assim, o foco no Processo de Fiscalização Rodoviária, que consiste na recolha de infrações de trânsito e tratamento de autos de contraordenação, tal como se demonstra na Figura 14, os Locais de Controlo de Velocidade (LCV), recolhem eventos de excesso de velocidade (infrações), nesses eventos, são recolhidas as provas fotográficas que identificam as matriculas dos veículos, permitindo obter os dados dos condutores, para processamento no Sistema de Contraordenações, gerando a notificação ao condutor (Auto de Contraordenação).

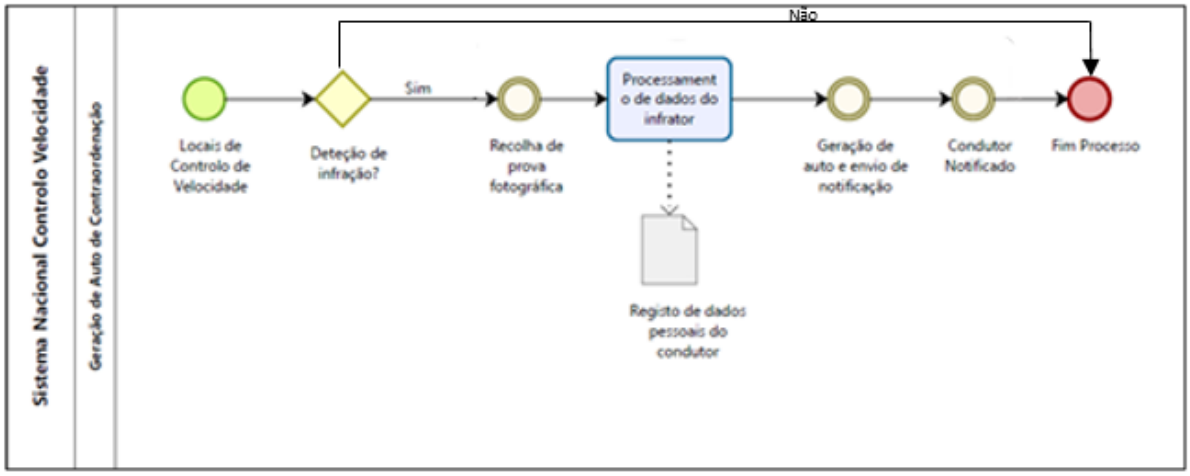

Figura 14 – Processo de Contraordenação Rodoviária

Neste sentido, e no âmbito da sua missão, a ANSR é detentora de uma quantidade relevante de informação, com constante transformação digital, desde a sua criação até à sua disponibilização e armazenamento, via Sistemas de Informação (SI). Esta informação tem um peso relevante por, da mesma, resultarem processos contraordenacionais e administrativos, bem como, matérias sensíveis e confidenciais resultantes desses processos.

A informação gerada no âmbito da componente de negócio principal da ANSR, i.e., o processo contraordenacional rodoviário, assume assim o peso de ativo com elevada relevância para esta autoridade do Ministério da Administração Interna (MAI), tornando-se necessária, a identificação de vulnerabilidades e ameaças, que possam originar a sua perda total ou parcial, através de acessos não autorizados à mesma.

No contexto laboral de teletrabalho derivado da pandemia mundial Covid-19, o Caso de Estudo irá utilizar um modelo de gestão de risco integrado pela ISO31000 e ISO27005, especificamente na sua componente de avaliação de **risco intrínseco**, dos ativos da organização, a ANSR, antes e depois de terem sido colocados em teletrabalho, numa determinada escala de classificação do nível do risco baixo, médio ou alto, para um período homólogo: janeiro a julho de 2019 e janeiro a julho de 2020.

Não foi encontrado um artigo científico específico, que cruzasse a Segurança de Informação com a pandemia Covid-19, numa perspetiva de análise e gestão de risco. No entanto, destaca-se o artigo científico *Developing a conceptual model for insider threat*, da base de dados de conhecimento cientifico Minerva da Universidade de Melbourne, verificando que o mesmo, contribuiu para correlacionar causas e consequências do foro psicossocial de colaboradores de organizações, na concretização de ciberataques internos a essas organizações. Foi aliás este artigo, a base para o inicio da investigação da presente dissertação, tendo presente que as motivações das ameaças internas das organizações, demonstradas no mesmo, eram em muito semelhantes às consequências psicossocias do teletrabalho em contexto pandemia Covid-19, nas organizações. O modelo descrito nesse artigo, não foi reproduzido na sua plenitude no caso de estudo retratado na presente dissertação, isto porque, alguns dados referenciados nesse modelo são de carater sensível (nomes de colaboradores e a sua situação clinica), assim, no que respeita aos dados recolhidos para a presente dissertação, não foram tratados dados pessoais dos colaboradores da ANSR, ou seja, dados que cruzem matéria de privacidade dos seus titulares, para além do que, o principal agente em matéria de tecnologia, segurança e monotorização, da infraestrutura tecnológica da ANSR, a Rede Nacional de Segurança Interna (RNSI), também por motivos de privacidade, não disponibiliza determinados dados (nomes dos utilizadores de rede) na caracterização da *insider threat*. Assim, à exceção de dados pessoais, todos os restantes dados recolhidos de eventos de *insider threat*, foram tratados, permitindo relacionar o artigo com o Caso de Estudo da presente dissertação, onde se realçam causas do foro psicossocial, que de certa forma potenciam ou podem potenciar vulnerabilidades dos colaboradores, colocando em risco os ativos das organizações.[26]

No caso específico da ANSR, foram recolhidas duas amostras de dados. A primeira amostra, identifica eventos de incidentes de segurança, registados no período de janeiro de 2019 a julho de 2020. A segunda amostra, identifica os Ativos no âmbito definido, i.e., quantidade de equipamentos TI (postos de trabalho) dos colaboradores da ANSR, colocados em regime de teletrabalho no início de 2020.

2. Aplicação do Modelo ao Caso de Estudo

Numa metodologia de gestão de risco existe sempre a perspetiva de continuidade, ou seja, um processo de melhoria contínua, onde há lugar a uma monotorização e revisão para avaliação se o processo continua responsivo aos desafios identificados através dos controlos de segurança aplicados, ou se precisa de ajustes e adaptações a esses controlos de segurança aplicados. Pese embora esta seja uma condição *sine qua non* do processo de gestão de risco, seja qual for a metodologia aplicada, numa primeira instância, existe lugar a um primeira avaliação do risco (*assessement*), i.e., a uma

primeira apreciação do risco na perspetiva de que ainda não foram aplicados quaisquer controlos de segurança, o cálculo do risco intrínseco dos ativos do âmbito [35], [40].

Será esta a perspetiva da aplicação do *modelo* identificada, i.e., a apreciação do risco num primeiro ponto de arranque da aplicação de um Modelo de Gestão de Risco Aplicado à Segurança de Informação, através de um Modelo Integrado ISO 31000/ISO 27005, no contexto Organizacional: Antes e depois da Pandemia Covid-19 e Regime de teletrabalho, de modo a apurar o risco intrínseco dos ativos do âmbito, ou seja, risco apurado na primeira avaliação, quando ainda não existem controlos de segurança aplicados. Tendo em conta o modelo a adaptar, conforme já referenciado na Figura 12 do Capítulo II, resultante da conjugação da ISO31000 com a ISO27005, nomeadamente:

Desta forma, iremos focar-nos em apurar o risco intrínseco dos ativos do âmbito, antes e depois da realidade teletrabalho. Assim, as fases do modelo aplicado a desenvolver neste ponto, serão as fases do *assessement* (ilustrado na Figura 13) aliado ao âmbito a aplicar:

- *Definição do Âmbito;*
- *Apreciação do Risco (Risk assessement pela 27005) que agrega as fases da ISO31000:*
    - *Identificação do risco;*
    - *análise do risco;*
    - *avaliação do risco.*

As restantes fases não serão alvo de análise na dissertação, verificando-se que para o efeito das mesmas se depreende uma continuidade e monotorização dos ativos após aplicadas medidas de segurança, ou seja, na fase de tratamento do risco, e esta não foi o alvo da investigação do Caso de Estudo, mas sim o apuramento do risco intrínseco dos ativos do âmbito.

CAPÍTULO V – Caso de Estudo: Avaliação do risco dos Processos da ANSR

1. Problema e Hipótese

Quando se fala de investigação científica, existem obrigatoriamente duas questões a analisar, "Qual é o meu problema?" e em resultado desta "O que devo fazer?" [16]. Nesta perspetiva, e tendo em conta a Definição do Problema, descrito no ponto 3 do Capítulo I, o ***Problema*** identificado na presente dissertação é: ***avaliação e monitorização do risco de Segurança de Informação, no contexto das novas formas de organização do trabalho***.

Sendo a hipótese apresentada, associada ao o aumento de eventos de incidentes de segurança, entre janeiro de 2019 e julho de 2020. Especificamente no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020. Assim, a **hipótese formulada** é**: *o modelo proposto na presente dissertação, de gestão de risco de Segurança de Informação adaptado a novas formas de organização do trabalho, vem permitir apurar o risco intrínseco das vulnerabilidades e ameaças, dos ativos da ANSR, em contexto de teletrabalho.***

2. Recolha e Análise de Dados

2.1. Recolha de Dados

Os dados utilizados na investigação repartem-se em duas amostras:

- **1ª Amostra**: Eventos (incidentes de segurança) registados no período de janeiro de 2019 a julho de 2020;
- **2ª Amostra**: Ativos identificados no âmbito definido (equipamentos TI dos colaboradores da ANSR) colocados em regime de teletrabalho no início de 2020.

2.1.1. 1ª Amostra - Eventos na Infraestrutura Tecnológica

A **1ª Amostra** de dados foi disponibilizada pela RNSI, extraídos de uma ferramenta de monotorização interna desta entidade do MAI que, por motivos de segurança, não será referenciada na presente dissertação. A extração de dados foi disponibilizada em formato Excel, dos quais se identificaram e adaptaram os campos do Apêndice 1

Todos os restantes dados referenciados foram extraídos de artigos científicos, devidamente mencionados.

2.1.2. 2ª Amostra - Ativos em Teletrabalho

A **2ª Amostra** de dados foi disponibilizada pelo Núcleo de Informática (NIF) da Divisão de Apoio e Desenvolvimento Organizacional (DADO) da ANSR, recolhidos através de inventário do NIF, representado em formato Excel, dos quais se identificaram e adaptaram os campos da Apêndice 2.

3. Análise de Dados

3.1. 1ª Amostra - Eventos na Infraestrutura Tecnológica

Entre janeiro de 2019 e julho de 2020, foram disponibilizados dados de eventos na infraestrutura tecnológica da ANSR, pela RNSI, onde se observou por tipo de ameaças, i.e., tipos de ataques, dos cerca de 1007 eventos registados (432 eventos em 2019 e 575 eventos em 2020), foram identificados 973 incidentes de segurança, identificados na Tabela 3 e Figura 15. A variação entre os períodos homólogos, primeiro semestre de 2019 e primeiro semestre de 2020, é notoriamente crescente em termos de incidentes identificados. Em julho de 2020 o total de incidentes de segurança superava o total de todo o ano de 2019. Este facto, coincide com o início do período pandémico (a partir de janeiro de 2020) e adesão das organizações ao teletrabalho.

Tabela 3 – Quantidade de incidentes de segurança registados a ANSR entre janeiro de 2019 e julho de 2020

Incidentes Registados	Ano		
Mês	2019	2020	Total Geral
JANEIRO	13	82	95
FEVEREIRO	16	34	50
MARÇO	29	82	111
ABRIL	16	58	74
MAIO	31	32	63
JUNHO	57	107	164
JULHO	16	155	171
AGOSTO	24		24
SETEMBRO	35		35
OUTUBRO	40		40
NOVEMBRO	41		41
DEZEMBRO	105		105
Total Geral	**423**	**550**	**973**

Podemos observar na Figura 15 a evolução dos incidentes de segurança, desde janeiro de 2019 a julho de 2020.

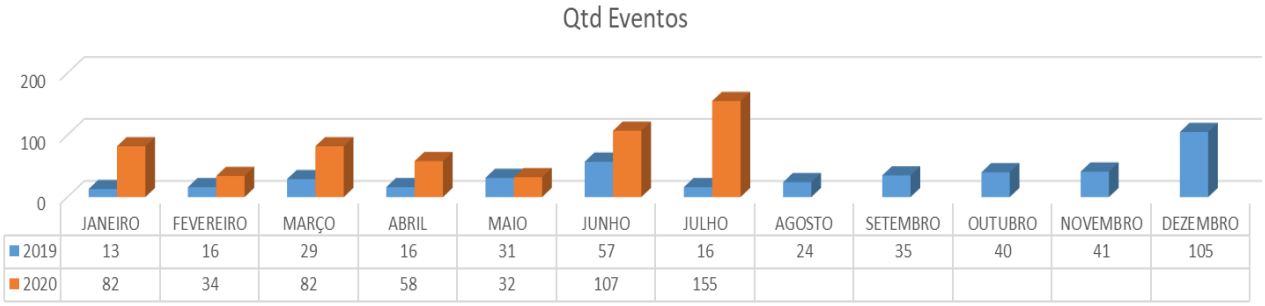

Figura 15 – Quantidade de incidentes de segurança registados na ANSR de janeiro de 2019 a julho de 2020

É preciso observar que os dados de 2019 dizem respeito a 12 meses, enquanto que os dados de 2020 apenas se reportam a 7 meses, pelo que, até final de 2020, muito provavelmente o número de incidentes de segurança será ainda mais elevado. Podemos, no entanto, concluir que no período homólogo de 7 meses de 2019 e de 2020, foi ultrapassada a quantidade de incidentes de segurança

de 2019 em praticamente mais de 300% dos registados em 2019 (registados 178 em 7 meses de 2019, registados 550 em 7 meses de 2020), conforme observado na Tabela 4.

Tabela 4 – Quantidade de incidentes de segurança registados na ANSR no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020

Incidentes Registados Ano / Mês	2019	2020	Total Geral
JANEIRO	13	82	95
FEVEREIRO	16	34	50
MARÇO	29	82	111
ABRIL	16	58	74
MAIO	31	32	63
JUNHO	57	107	164
JULHO	16	155	171
Total Geral	**178**	**550**	**728**

A partir deste momento iremos evidenciar a análise de dados para a investigação, apenas no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020, com a particularidade de que só foi possível recolher dados até julho de 2020. Assim, na Figura 16 focamos o período homólogo entre 2019 e 2020, para comparação.

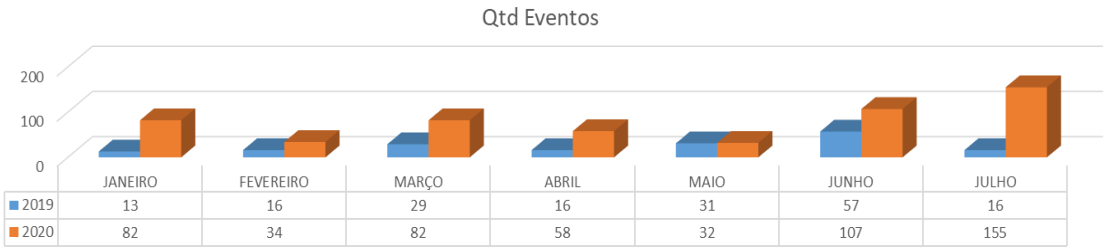

Figura 16 – Quantidade de Incidentes de segurança registados na ANSR no período homólogo janeiro a julho e 2019 e janeiro a julho de 2020

Dos 728 incidentes de segurança registados no período homólogo entre janeiro de 2019 a julho de 2020, demonstra-se na Tabela 5, a quantidade desses incidentes por tipo de ataque. O tipo de ataques evidenciados, nesta tabela, estão relacionados com tipos de *phishing* e são muitas vezes concretizados através de técnicas de Engenharia Social, principalmente ataques *Cross Site Scripting XSS* e *SQL Injection*, permitindo acesso e manipulação de dados (informação) individuais e corporativos, por pessoas não autorizadas e com fins maliciosos [41].

Tabela 5 – Quantidade de incidentes de segurança registados na ANSR por tipo de Ataque no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020

Contagem de id DO EVENTO	Rótulos de Coluna		
Tipo de Ataque	2019	2020	Total Geral
PHISHING	16	20	36
SEXTORTION		2	2
SPAM	4	3	7
SQL INJECTION		49	49
DOS/DDOS	76	69	145
JAVASCRIPT INJECTION	13	213	226
MALWARE	69	194	263
Total Geral	**178**	**550**	**728**

Assim, na Figura 17 salientamos o período homólogo entre 2019 e 2020, para comparação da evolução dos incidentes de segurança por tipo de ataque. No período homólogo janeiro a julho de 2019 e janeiro a julho de 2020, observou-se um aumento significativo dos tipos de ataque: Malware, SQL Injection e JavaScript injection.

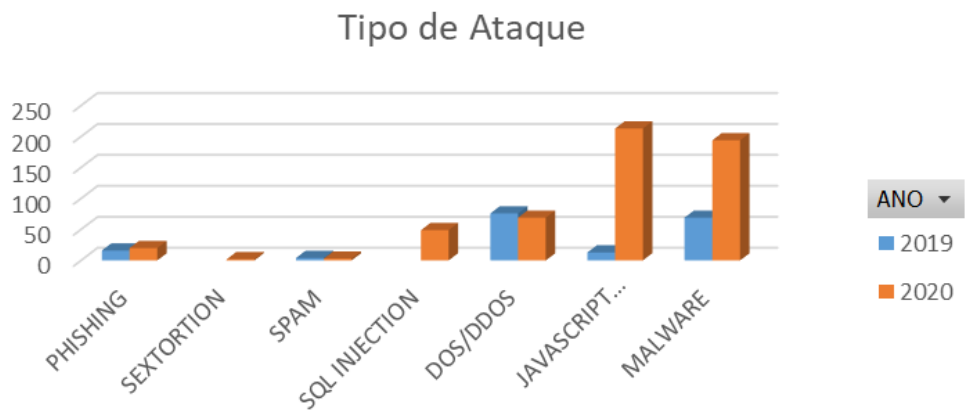

Figura 17 – Quantidade de incidentes de segurança registados na ANSR por tipo de Ataque no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020

Na Tabela 6 conseguimos observar a quantidade de ataques, no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020, por ponto de entrada dos mesmos, onde se observa que houve um aumento significativo de ataques através de origem WEB que se referem a vários Sites (não corporativos) acedidos por colaboradores da ANSR, e desses pontos de entrada os ataques que mais aumentaram foram: *Malware*, *SQL* Injection e *JavaScript* Injection (*Cross-Site Scripting XSS*). Na Figura 18 conseguimos ver graficamente esta acentuação de ataques de 2019 para 2020.

Tabela 6 – Quantidades de incidentes de segurança registados na ANSR por ponto de entrada do Ataque no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020

PONTO ENTRADA ATAQUE	2019	2020	Total Geral
DOWNLOAD	**6**	**7**	**13**
MALWARE	6	7	13
EMAIL	**63**	**42**	**105**
MALWARE	46	19	65
PHISHING	13	20	33
SPAM	4	3	7
PORTAL CONTRAORDENAÇÕES	**34**	**2**	**36**
DOS/DDOS	34	2	36
SITE ANSR		**17**	**17**
DOS/DDOS		17	17
WEB	**75**	**482**	**557**
DOS/DDOS	42	50	92
JAVASCRIPT INJECTION	13	213	226
MALWARE	17	168	185
PHISHING	3		3
SEXTORTION		2	2
SQL INJECTION		49	49
Total Geral	**178**	**550**	**728**

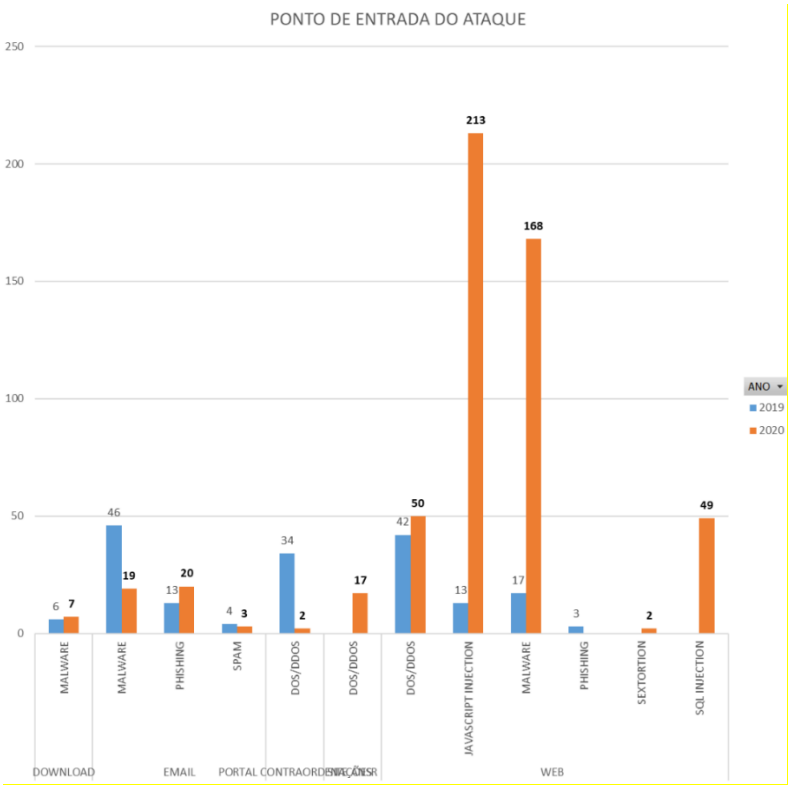

Figura 18 – Quantidade de incidentes de segurança registados na ANSR por ponto de entrada do ataque no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020

Outra observação pertinente foi que, conforme demonstrado na Tabela 7, no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020, enquanto que em 2019 a maior parte dos incidentes de segurança ocorreu no período laboral (9:00 às 18:00), já em 2020 existe uma ocorrência quase idêntica dentro e fora do período laboral, esta situação resulta claramente de uma passagem a regime de teletrabalho onde os horários de trabalho tendem a alargar-se e até mesmo a ficarem desajustados e difíceis de padronizar.

Tabela 7 – Quantidade de incidentes de segurança registados na ANSR dentro e fora do período laboral (9:00 às 18:00) no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020

PERIODO	2019	2020	Total Geral
Entre as 9:00 e as 18:00	146	273	419
Entre as 18:01 e as 08:59	32	277	309
Total Geral	**178**	**550**	**728**

Na Figura 19 podemos observar a representatividade (%) de incidentes de segurança, no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020, em que se verifica que, em 2019 a maior ocorrência (cerca de 82%) ocorria dentro do período laboral (9:00 às 18:00), já em 2020 a ocorrência de incidentes dá-se de uma forma quase equilibrada, dentro e fora do período laboral.

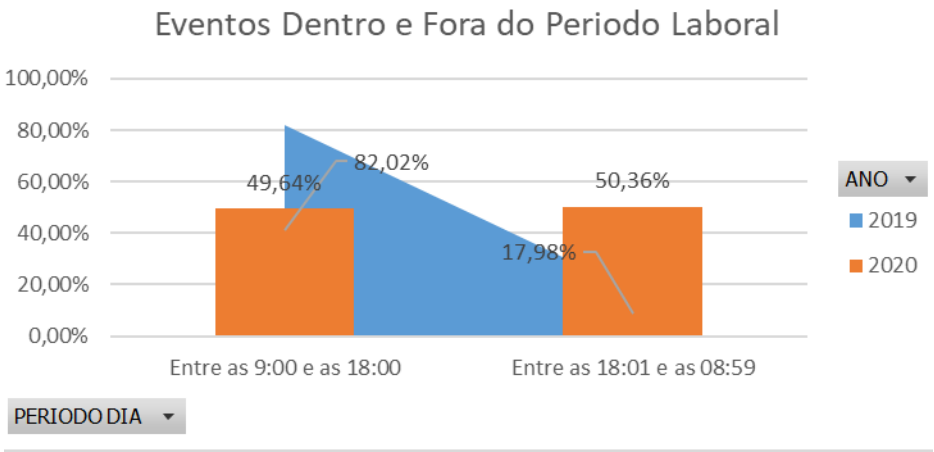

Figura 19 – Incidentes de segurança registados na ANSR dentro e fora do período laboral (9:00 às 18:00) no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020

3.2. 2ª Amostra - Ativos em Teletrabalho

Foram observadas as seguintes dimensões afetas aos colaboradores da ANSR:

a. Perfil de Responsabilidade

- Número de colaboradores, por perfil de responsabilidade, alocados em regime de teletrabalho, antes e depois da pandemia, no período homólogo entre

janeiro de 2019 a julho de 2019 e janeiro de 2020 a julho de 2020, com ativos móveis (equipamentos que contribuem para o ativo primário) quantidades demonstradas na Tabela 8.

Tabela 8 – Quantidade e % de Ativos em teletrabalho antes e depois da pandemia por perfil de responsabilidade no período homólogo janeiro a julho de 2019 e janeiro e julho de 2020

	Janeiro 2019 a Julho 2019				Janeiro 2020 a Julho 2020			
RESPONSABILIDADE	QTD Antes Pandemia Teletrabalh	% Antes Pandemia Teletrabalh	QTD Antes Pandemia Local	% Antes Pandemia Local	QTD Durante Pandemia Teletrabalho	% Durante Pandemia Teletrabalho	QTD Durante Pandemia Local	% Durante Pandemia Local
A.Presidência	4	2,25%	0	0,00%	4	2,25%	0	0,00%
B.Dirigente	8	4,49%	0	0,00%	8	4,49%	0	0,00%
C.Técnico/a Perfil Coordenação	11	6,18%	0	0,00%	11	6,18%	0	0,00%
D.Técnico/a Perfil Operacional	0	0,00%	155	87,08%	155	87,08%	0	0,00%
Σ	23	12,92%	155	87,08%	178	100,00%	0	0,00%

Antes do período da pandemia estavam alocados 23 ativos a teletrabalho e 155 a trabalho local, já depois da pandemia ficaram alocados a teletrabalho os 178 ativos, existindo um aumento de 87,08% de ativos alocados em teletrabalho no período da pandemia, entre janeiro 2020 a julho 2020.

b. Tipo de Vínculo

Para além do tipo de responsabilidade dos titulares dos ativos, foi também apurado o tipo de vínculo destes à ANSR, onde se verificam os valores na Tabela 9.

Tabela 9 – Tipo de Vínculo dos Ativos em Teletrabalho

Tipo de Vinculo	Qtd	%
COLABORADOR ANSR	138	77,53%
PRESTADOR SERVIÇO	40	22,47%
Total Geral	**178**	**100,00%**

Cerca de 22% de ativos pertencem a vínculos externos (prestadores de serviço) e cerca de 78% de ativos pertencem a colaboradores da ANSR, i.e., a grande maioria são colaboradores da ANSR, observe-se na Figura 20 os valores apurados. Esta condição não se altera independentemente do período posterior ou anterior à pandemia, ou seja, mantém-se nos períodos homólogos em análise.

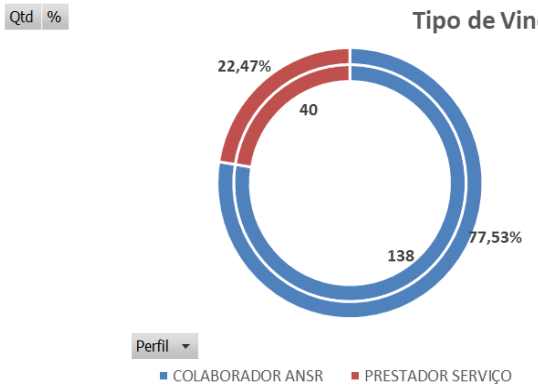

Figura 20 – Tipo de Vínculo dos Ativos em Teletrabalho

c. Área

Observa-se também, pelos dados recolhidos, as seguintes quantidades de ativos distribuídos por áreas, representados na Tabela 10.

Tabela 10 – Área afeta aos Ativos em Teletrabalho

AREA	Qtd	%
A.ALTA DIREÇÃO	12	6,74%
B.JURIDICA	59	33,15%
C.RECURSOS HUMANOS	5	2,81%
D.FINANCEIRA E CONTRATUAL	14	7,87%
E.TÉCNICA	76	42,70%
F.ADMINISTRATIVA	12	6,74%
Total Geral	**178**	**100,00%**

Na Figura 21 é evidenciada a representação percentual das quantidades de ativos distribuídos por áreas.

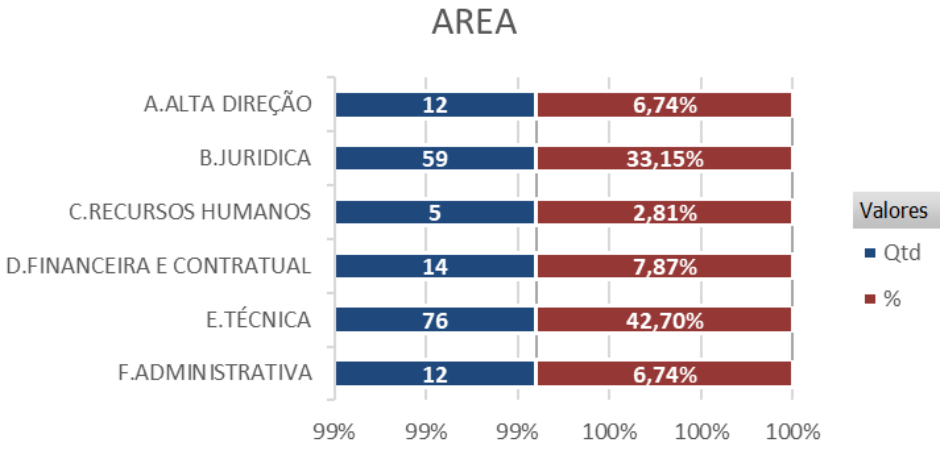

Figura 21 – Área afeta aos Ativos em Teletrabalho

Esta condição também não se altera independentemente do período posterior ou anterior à pandemia, ou seja, mantém-se nos períodos homólogos em análise.

4. Definição do Âmbito

Aplicando a metodologia definida no ponto 1., do Capitulo III, a ANSR, tem uma estrutura orgânica, em que cada unidade e divisão fica sob a autoridade de um gestor de divisão responsável pelas decisões estratégicas, administrativas e operacionais de sua unidade, que, por sua vez, respondem perante as decisões estratégicas delineadas pela Presidência da ANSR [49]. Neste âmbito estrutural, o modelo de gestão de risco implementado, deve dar resposta à decisão superior da ANSR (Presidência), para a qual contribuem também os responsáveis das unidades e divisões respetivas.

Esta definição, e levando em conta os Ativos (equipamentos portáteis) em contexto de teletrabalho da ANSR derivado da pandemia Covid-19, que acedem a informação classificada da ANSR, diretamente associada à identidade, missão, valores e objetivos estratégicos da organização, tendo em conta a informação sensível (dados pessoais) envolvidos no processo de contraordenação rodoviária demonstrado na Figura 14, do n.º1 do Capitulo IV, temos assim o Âmbito ilustrado na Figura 22.

Figura 22 – Âmbito do modelo de aplicação do Anexo A1 da 27005 e características da organização pelo Decreto Regulamentar n.º28/2012 [40], [49]

5. Apreciação do Risco - Identificação do Risco

Conforme definido no ponto 3.2., do Capítulo V, vamos aplicar as dimensões afetas aos colaboradores da ANSR em regime de teletrabalho:

a. **Perfil de Responsabilidade;**
b. **Tipo de Vínculo;**
c. **Área.**

Tendo sido apuradas as dimensões, obtemos o inventario de ativos representado na Tabela 11, bem como as classes dos ativos na Tabela 12:

Tabela 11 – Inventário de Ativos dimensões dos Ativos secundários apurados

Dimensão	Qtds Ativos
Perfil de Responsabilidade	
A.Presidência	4
B.Dirigente	8
C.Técnico Coordenação	11
D.Técnico Operacional	155
Tipo Vinculo	
Colaborador ANSR	138
Prestador de Serviço	40
Área	
A.ALTA DIREÇÃO	12
B.JURIDICA	59
C.RECURSOS HUMANOS	5
D.FINANCEIRA E CONTRATUAL	14
E.TÉCNICA	76
F.ADMINISTRATIVA	12

Tabela 12 – Classe de Ativos secundários

CLASSES ATIVOS	PERFIL RESPONSABILIDADE	TIPO VINCULO	ÁREA	Qtds
ATIVO I	A.PRESIDÊNCIA	COLABORADOR ANSR	ALTA DIREÇÃO	4
ATIVO II	B.DIRIGENTE	COLABORADOR ANSR	ALTA DIREÇÃO	8
ATIVO III	C. + D. TÉCNICO	COLABORADOR ANSR E PRESTADOR SERVIÇO	RECURSOS HUMANOS, FINANCEIRA E CONTRATUAL, TÉCNICA, ADMINISTRATIVA.	166

5.1. Valorização dos Ativos (Matriz de Impacto)

Assim, no contexto Organizacional em que a ANSR se insere, e de acordo com as componentes definidas no ponto 3.2., do Capítulo V, serão levadas em conta para a definição de uma Matriz de Limites de Impacto, os seguintes componentes:

a. **Níveis de Impacto** - Estabelecemos os níveis de impacto de 1 a 5, para os diferentes valores de cada linha orientadora (b.) de análise de impacto de concretização da ameaça, com o seguinte critério:

   - ✓ **Nível 1** Sem Impacto no processo core da ANSR e informação classificada no mesmo (ativos primários);
   - ✓ **Nível 2** Impacto reduzido no processo core da ANSR e informação classificada no mesmo (ativos primários);
   - ✓ **Nível 3** Impacto significativo no processo core da ANSR e informação classificada no mesmo (ativos primários);
   - ✓ **Nível 4** Impacto grave no processo core da ANSR e informação classificada no mesmo (ativos primários);
   - ✓ **Nível 5** Ameaça à sobrevivência do Negócio da ANSR.

b. Linhas Orientadoras - Estabelecemos as linhas orientadoras de análise de impacto de concretização da ameaça, do seguinte modo:

   - ✓ **Perdas Financeiras** - Perda direta de receita resultante da aplicação do processo contraordenacional, ou elevados custos para recuperação de receita do processo contraordenacional.
   - ✓ **Esforço de Operações** - Incremento dos esforços de produção, esforços operacionais, esforços associados à contratação de Recursos Humanos adicionais, ou para recuperação de imagem.
   - ✓ **Reputação e Imagem** - Perda de confiança dos cidadãos, público em geral, partes interessadas, entidades reguladoras, entidades de supervisão e/ou colaboradores.
   - ✓ **Legais/Regulamentares** - Sujeição a potenciais investigações, multas ou penalidades por parte de entidades reguladoras/governamentais, sanções contratuais e/ ou processos em tribunal.
   - ✓ **Envolvimento da Gestão de Topo da organização** - Envolve diretamente a Gestão de Topo influenciando o processo de tomada de decisão, seja a nível estratégico de investimentos e/ou conceção e desenvolvimento de novos serviços.

c. **Matriz de Limites de Impacto por Valores de Linhas Orientadoras para a avaliação de impacto -** Com base nos níveis de impacto definidos em (a.) relacionados com as linhas orientadoras de análise de impacto definidas em (b.), estabelece-se a seguinte Matriz de limites orientadores de avaliação de impacto (Tabela 13):

Tabela 13 – Matriz de Impacto dos Ativos secundários apurados

a. Níveis de Impacto	b. Linhas Orientadoras				
IMPACTO	**PERDAS FINANCEIRAS**	**ESFORÇO DE OPERAÇÕES**	**REPUTAÇÃO E IMAGEM**	**LEGAISE REGULAMENTARES**	**EMVOLVIMENTO DA GESTÃO DE TOPO DA ORGANIZAÇÃO**
1 Sem Impacto nos serviços prestados	Perdas até 100.000,00€	Sem impacto significativo no esforço operacional	Afeta negativamente as relações com outras partes da organização. Sem impacto nos meios de comunicação.	Sem impacto significativo no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Resolução de incidentes ao nível das equipas técnicas, os processos afetados não são estratégicos para a organização.
2 Impacto reduzido nos serviços prestados	Perdas até 1.000.000,00€	Impacto reduzido no esforço operacional	Afeta negativamente as relações com o público e com outras organizações no meio. Atenção pontual nos meios de comunicação, mas sem por em causa a imagem da organização.	Impacto reduzido no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Resolução de incidentes ao nível das equipas técnicas, com necessidade de esclarecimentos dos diretores de primeira linha, os processos afetados não são estratégicos para a organização.
3 Impacto significativo nos serviços prestados	Perdas até 5.000.000,00€	Impacto significativo no esforço operacional (sobrecarga de recursos).	Afeta negativamente as relações com o público e com outras organizações. Atenção adversa nos meios de comunicação, mas sem por em causa a imagem da Organização.	Impacto significativo no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Envolvimento direto dos diretores de primeira linha na resolução de incidentes, a Gestão de Topo da organização é notificada, os processos afetados não são estratégicos para a Organização.
4 Impacto grave nos serviços prestados	Perdas até 10.000.000,00€	Grande impacto no esforço operacional, alocação de horas extra aos recursos.	Publicidade Negativa passa nos meios de comunicação, suscetível de colocar em causa a imagem da organização.	Grande impacto no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Requer decisão e gestão pontuais por parte da Gestão de Topo da Organização, os processos afetados são estratégicos para a organização.
5 Ameaça à sobrevivência do Negócio / Prestação de Serviço	Perdas superiores a 10.000.000,00€ ou perdas suficientes para impedir a continuidade do negócio	Impacto Catastrófico no esforço operacional (para além de alocação de horas extra aos recursos, existe a necessidade de suspender atividades diárias).	Publicidade Negativa passa nos meios de comunicação com grande repercussão, colocando em causa a imagem da organização.	Impacto catastrófico no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Requer envolvimento ativo da Gestão de Topo da Organização, os processos afetados são estratégicos para a organização.

Os valores da Tabela 13, relativamente às perdas financeiras, são referencias mensuráveis tendo em conta a receita anual da organização.

5.1.1. Análise do impacto sobre os Ativos

É necessário que a avaliação para cada ativo, das classes identificadas na Tabela 12, esteja de acordo com a Matriz de impacto definida na Tabela 13, fazendo parte desta avaliação a perspetiva de que esses ativos não têm ainda controlos de segurança aplicados, e assim sendo, o impacto que terão caso se concretizem ameaças a esses ativos que coloquem em causa os princípios da Segurança de Informação que contribuem para os ativos principais da ANSR, relacionados com a confidencialidade, integridade, disponibilidade, autenticidade e não repúdio, e a legitimidade da informação (Anexo A).

O valor máximo da matriz associada a cada ativo dar-nos-á o valor do mesmo; no entanto, se outros ativos dependerem desse, o valor do ativo que estamos a analisar passará a ser o valor máximo dos ativos dependentes deste.

No Caso de Estudo aqui referido, identificamos três Classes de Ativos (postos de trabalho), em função dos três Perfis de Responsabilidade existentes na ANSR, conforme demonstrado na Tabela 12. Assim, tendo em conta a matriz de impacto definida na Tabela 13, caso se concretizem ameaças que coloquem em causa a confidencialidade, integridade, disponibilidade, autenticidade e não repúdio, e legitimidade da informação dos ativos principais do âmbito, temos a seguinte escala de ponderação demonstrada na Tabela 14, para cenários (coluna Escala da Tabela 14) identificados, com base em histórico de incidentes de segurança de uma equipa de tecnologias de informação, da ANSR:

Tabela 14 – Matriz de Ponderação de Nível de Impacto pelas Linhas Orientadoras da Matriz de Impacto dos Ativos secundários apurados

Incidente	Escala	Nível Impacto apurado de acordo com linhas orientadoras tabela 13		
		Classe Ativo I	Classe Ativo II	Classe Ativo III
Disponibilidade	Falha na disponibilidade até 15 minutos	1	1	1
	Falha na disponibilidade até 3 horas	2	2	1
	Falha na disponibilidade até 1 dia	2	2	2
	Destruição Parcial de Informação	4	4	3
	Destruição Total de Informação	5	5	4
Integridade	Modificação não publicada	1	1	1
	Modificação sem controlo de versões	2	1	1
	Modificação não autorizada	3	3	2
	Perda parcial de histórico de versões	4	4	3
	Perda total de histórico de versões	5	5	4
Confidencialidade	Informação não classificada	1	1	1
	Informação confidencial acedida por pessoa interna não autorizada	4	4	3
	Informação confidencial acedida por pessoa externa não autorizada	5	5	4
	Divulgação interna de informação confidencial	3	3	2
	Divulgação externa de informação confidencial	5	5	4
Autenticidade e Não Repúdio	Informação sem fonte de autenticidade	2	2	2
	Alteração por negligência de autenticidade da Informação	2	2	2
	Alteração propositada de autenticidade da Informação	3	3	3
	Divulgação interna de informação sem autenticidade	4	4	3
	Divulgação externa de informação sem autenticidade	5	5	4
Legitimidade	Evidencia de não conformidade com regulamentos internos	4	4	4
	Evidencia de não conformidade normativa ou regulamentar	4	4	4
	Evidencia de não conformidade legal de acordo com legislação aplicada à área de negocio da organização	5	5	4
	Dados pessoais acedidos, ou, sobre alvo de tratamento sem autorização dos titulares	5	5	4
	Dados sensíveis (dados saúde, etc…) acedidos, ou, sobre alvo de tratamento sem autorização dos titulares	5	5	4

Podemos assim verificar que o valor máximo da matriz associada a cada ativo (Ativo I, Ativo II e Ativo III) dar-nos-á o valor de cada um dos ativos em análise, assim poderemos dizer, ainda na fase em que não existem controlos de Segurança de Informação aplicados, que o valor de impacto sobre:

- ✓ Ativo I Valor 5;
- ✓ Ativo II Valor 5;
- ✓ Ativo III Valor 4.

Os Ativos assumem, assim, o valor máximo do nível de impacto apurado de acordo com as linhas orientadoras da Matriz de impacto dos ativos secundários apurados Tabela 14.

5.2. Apreciação do Risco - Análise do Risco

A fase de Apreciação do Risco resulta de um processo global de identificação, análise e avaliação do mesmo. Passamos assim a demonstrar de uma forma integrada estas fases, tendo em conta o âmbito dos ativos. Importa antes de tudo distinguir o que são ameaças e o que são vulnerabilidades [40]:

- ✓ **AMEAÇA (ISO27005 8.2.3)**, representa um possível ataque interno ou externo a determinado alvo, com intenção de provocar danos totais ou parciais nesse alvo.

- ✓ **VULNERABILIDADE (ISO27005 8.2.5)**, representa alguma fragilidade de determinado alvo, que possa ser explorada por uma ameaça de modo a provocar maior impacto num determinado ataque, ou seja, conteúdos não protegidos, ou com reduzida proteção, ou com proteção desatualizada e que não acompanham as ameaças atuais.

- ✓ **VEROSSEMELHANÇA (ISO27005 8.2.1),** representa a probabilidade de determinado evento acontecer, com base no histórico de eventos em determinado período.

5.2.1. Identificação das Ameaças

Conforme o âmbito identificado no ponto 4. do presente Capitulo V, bem como conforme a definição de ameaça identifica no ponto 3.2., do Capitulo III, iremos focar-nos nas ameaças com recurso a engenharia social, descritas no Anexo C da ISO27005, nomeadamente [40]:

Insiders threat (colaboradores da organização com intenção maliciosa ou negligente de provocar danos à organização)

O valor da ameaça de cada ativo será medido, obtendo o número total de eventos com a causa em determinada ameaça, ou % de ocorrências desse evento) sobre um ativo, em determinado período, tendo em conta os eventos apurados no período homólogo no ponto 3. Análise de Dados do presente Capítulo V, obtemos o resumo na seguinte Tabela 15:

Tabela 15 – Quantidade e % de eventos por tipo de Ataque apurados nos períodos homólogos janeiro a julho de 2019 e janeiro a julho de 2020

	2019		2020		Total QtdEventos	Total %Eventos
Tipo de Ataqu	QtdEventos	%Eventos	QtdEventos	%Eventos		
PHISHING	16	8,99%	20	3,64%	36	4,95%
SEXTORTION		0,00%	2	0,36%	2	0,27%
SPAM	4	2,25%	3	0,55%	7	0,96%
SQL INJECTION		0,00%	49	8,91%	49	6,73%
DOS/DDOS	76	42,70%	69	12,55%	145	19,92%
JAVASCRIPT INJECTION	13	7,30%	213	38,73%	226	31,04%
MALWARE	69	38,76%	194	35,27%	263	36,13%
Total Geral	**178**	**100,00%**	**550**	**100,00%**	**728**	**100,00%**

Se aplicarmos uma definição das seguintes classificações para os períodos homólogos de janeiro a julho de 2020:

- ✓ **Baixa (B):** verificados menos de 200 eventos de ataques aos ativos num período => 7 meses;
- ✓ **Média (M):** verificados menos de 300 eventos de ataques aos ativos num período => 7 meses
- ✓ **Alta (A):** verificados pelo menos 400 eventos de ataques aos ativos num período => 7 meses

Uma vez valorizadas as ameaças para cada um dos ativos, caso um deles seja alvo de várias ameaças, o valor de ameaça do ativo será o maior valor de todas as suas ameaças.

Pelos valores apurados na Tabela 15 obtemos a seguinte classificação da ameaça para os ativos do âmbito nos períodos homólogos:

Antes da Pandemia janeiro 2019 a julho 2019 (178 eventos)

- ✓ Ameaça Baixa.

No decorrer da Pandemia janeiro 2020 a julho 2020 (550 eventos)

- ✓ Ameaça Alta.

5.2.2. Identificação das Vulnerabilidades

Conforme o âmbito identificado no ponto 4. do presente Capitulo V, bem como conforme a definição de vulnerabilidade identificada no ponto 3.2., do Capitulo III, tendo em conta o facto dos Ativos estarem em teletrabalho sem supervisão por perfis de responsabilidade da ANSR, iremos focar-nos na vulnerabilidade, descrita no Anexo D da ISO27005, nomeadamente [40]:

- ✓ **Pessoal**
  - Trabalho não supervisionado por perfis de responsabilidade da organização;

As vulnerabilidades identificadas devem levar em conta a possibilidade de favorecer a ação de determinada ameaça, tendo em conta a probabilidade de que possa ocorrer o pior cenário possível.

O valor da vulnerabilidade de cada ativo será medido, obtendo a percentagem da vulnerabilidade através do número de ativos que apresentam determinada vulnerabilidade em determinado período, assim, levando em conta as Tabela 16 e Tabela 17, nos períodos homólogos:

- **Janeiro 2019 a julho 2019** temos 12,92% dos ativos em teletrabalho;
- **Janeiro 2020 a julho 2020** temos 100% dos ativos em teletrabalho;

Tabela 16 – Quantidade e % de Ativos em teletrabalho antes e depois da pandemia por Perfil de Responsabilidade no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020

	Janeiro 2019 a Julho 2019				Janeiro 2020 a Julho 2020			
RESPONSABILIDADE	QTD Antes Pandemia Teletrabalh	% Antes Pandemia Teletrabalh	QTD Antes Pandemia Local	% Antes Pandemia Local	QTD Durante Pandemia Teletrabalho	% Durante Pandemia Teletrabalho	QTD Durante Pandemia Local	% Durante Pandemia Local
A.Presidência	4	2,25%	0	0,00%	4	2,25%	0	0,00%
B.Dirigente	8	4,49%	0	0,00%	8	4,49%	0	0,00%
C.Técnico/a Perfil Coordenação	11	6,18%	0	0,00%	11	6,18%	0	0,00%
D.Técnico/a Perfil Operacional	0	0,00%	155	87,08%	155	87,08%	0	0,00%
Σ	23	12,92%	155	87,08%	178	100,00%	0	0,00%

Tabela 17 – Classe de Ativos secundários apurados

CLASSES ATIVOS	PERFIL RESPONSABILIDADE	TIPO VINCULO	ÁREA	Qtds
ATIVO I	A.PRESIDÊNCIA	COLABORADOR ANSR	ALTA DIREÇÃO	4
ATIVO II	B.DIRIGENTE	COLABORADOR ANSR	ALTA DIREÇÃO	8
ATIVO III	C. + D. TÉCNICO	COLABORADOR ANSR E PRESTADOR SERVIÇO	RECURSOS HUMANOS, FINANCEIRA E CONTRATUAL, TÉCNICA, ADMINISTRATIVA.	166

iremos assumir que a vulnerabilidade ocorreu a 100% durante o período de janeiro a julho de 2020 e a 12,92% durante o período homólogo de 2019, portanto nas probabilidades infra definidas iremos assumir que a probabilidade de ocorrência desta vulnerabilidade em 2020 é **Alta** e em 2019 era **Baixa**.

- ✓ **Baixa (B):** Probabilidade de ocorrência de determinada vulnerabilidade sobre determinado ativo no espaço de 7 meses =< 30%;

- ✓ **Média (M):** 30% < Probabilidade de ocorrência no espaço de 7 meses < 70%;

- ✓ **Alta (A):** Probabilidade de ocorrência no espaço de 7 meses => 70%.

5.3. Apreciação do Risco – Avaliação do Risco

5.3.1. Cálculo do Risco Intrínseco

O Risco Intrínseco é o risco apurado numa fase anterior a aplicação de qualquer tipo de medidas de segurança, ou seja, é o risco que os ativos têm de per si, em função das ameaças e vulnerabilidades que lhes são aplicáveis. Como é o caso do primeiro *assessement* que estamos a realizar na presente dissertação. Assim, de acordo com o definido no ponto 3.3., do Capítulo III, bem como com o valor do impacto dos ativos apurado no ponto 5.1. do presente Capítulo V, temos os seguintes valores de impacto por Ativo:

- ✓ Ativo I Valor de impacto 5;
- ✓ Ativo II Valor de impacto 5;
- ✓ Ativo III Valor de impacto 4.

Estes valores não se alteram antes e após a pandemia, ou seja, é o valor de impacto que cada ativo representa para a organização tendo em conta o âmbito definido e as vulnerabilidades e ameaças identificadas.

Sabemos também que, pela definição das escalas de ameaças e pela definição de escalas de vulnerabilidades dos pontos 5.2.1. e 5.2.2., do presente Capítulo V, a vulnerabilidade apurada é alta para os ativos em 2020 e baixa para os ativos em 2019.

Assim, obtém-se os seguintes cenários:

a. 2019
   - ✓ 2,25% pertencem a Ativo I ameaça Baixa;
   - ✓ 4,49% pertencem a Ativo II ameaça Baixa;
   - ✓ 6,18% pertencem a Ativo III ameaça Baixa.
   - ✓ Vulnerabilidade Baixa por apenas 12,92%, dos ativos estarem no período identificado em regime de teletrabalho sem supervisão de perfis de responsabilidade.
b. 2020
   - ✓ 2,25% pertencem a Ativo I ameaça Alta;
   - ✓ 4,49% pertencem a Ativo II ameaça Alta;
   - ✓ 93,26% pertencem a Ativo III ameaça Alta;
   - ✓ Vulnerabilidade Alta por todos os ativos estarem no período identificado em regime de teletrabalho sem supervisão de perfis de responsabilidade.

Define-se a seguinte escala de risco, o risco é medido numa escala de 0 a 7, e obtido pela conjugação da matriz Tabela 18 (2019) e Tabela 19 (2020) entre os valores das ameaças e vulnerabilidades dos ativos do âmbito, em que:

- ✓ Baixo Risco 0 a 2
- ✓ Médio Risco 3 a 5
- ✓ Alto Risco 6 a 7

Tabela 18 – Matriz de Risco Intrínseco 2019

	Ameaça	Baixa			Média			Alta		
	Vulnerabilidade	B	M	A	B	M	A	B	M	A
Valor do Impacto sobre o Ativo segundo matriz Tabela 13	0	0	1	2	0	1	2	0	1	2
	1	1	2	3	1	2	3	1	2	3
	2	2	3	4	2	3	4	2	3	4
	3	3	4	5	3	4	5	3	4	5
	4 (valor Ativo III Ameaça Baixa Vulnerabilidade Baixa)	**4**	5	6	4	5	6	4	5	6
	5 (valor Ativo I Ameaça Baixa Vulnerabilidade Baixa)	**5**	6	7	5	6	7	5	6	7
	5 (valor Ativo II Ameaça Baixa Vulnerabilidade Baixa)	**5**	6	7	5	6	7	5	6	7

Assim, segundo a Matriz de Cálculo do Risco Intrínseco 2019 (Tabela 18), temos os valores Risco Intrínseco:

RAtivo I = **5**

RAtivo II = **5**

RAtivo III = **4**

Tratando-se o Risco Total Intrínseco de uma variável ordinal, iremos apurar para 2019 a mediana dos valores de risco intrínseco de todos ativos, assim na ordem de valores crescente 4, 5 e 5, obtemos o valor de mediana: **Md** = **5** **(III - 1)**

Em que:

RAtivoI Risco Intrínseco do Ativo I apurado na tabela 18

RAtivoII Risco Intrínseco do Ativo I apurado na tabela 18

RAtivoIII Risco Intrínseco do Ativo I apurado na tabela 18

O Risco Intrínseco apurado dos ativos em 2019 é de **Médio Risco** de acordo com a escala definida de 0 a 7.

Tabela 19 – Matriz de Risco Intrínseco 2020

	Ameaça	Baixa			Média			Alta		
	Vulnerabilidade	**B**	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
Valor do Impacto sobre o Ativo segundo matriz Tabela 13 –	0	0	1	2	0	1	2	0	1	2
	1	1	2	3	1	2	3	1	2	3
	2	2	3	4	2	3	4	2	3	4
	3	3	4	5	3	4	5	3	4	5
	4 (valor Ativo III Ameaça Alta Vulnerabilidade Alta)	4	5	6	4	5	6	4	5	**6**
	5 (valor Ativo I Ameaça Alta Vulnerabilidade Alta)	5	6	7	5	6	7	5	6	**7**
	5 (valor Ativo II Ameaça Alta Vulnerabilidade Alta)	5	6	7	5	6	7	5	6	**7**

Assim, segundo a Matriz de Cálculo do Risco Intrínseco 2020 (Tabela 19), temos os valores Risco Intrínseco:

RAtivo I = **7**

RAtivo II = **7**

RAtivo III = **6**

Tratando-se o Risco Total Intrínseco de uma variável ordinal, iremos apurar para 2020 a mediana dos valores de risco intrínseco de todos ativos, assim na ordem de valores crescente 6, 7 e 7, obtemos o valor de mediana: **Md** = **7** **(III - 2)**

Em que:

RAtivoI Risco Intrínseco do Ativo I apurado na tabela 19

RAtivoII Risco Intrínseco do Ativo I apurado na tabela 19

RAtivoIII Risco Intrínseco do Ativo I apurado na tabela 19

O Risco Intrínseco apurado dos ativos em 2020 é de **Alto Risco** de acordo com a escala definida de 0 a 7.

5.3.2. Definição do Risco Aceitável

À data da presente dissertação a gestão de topo da ANSR, não tinha ainda definido o nível de riscos que está disposta a assumir, denominado “limite de risco”, sendo necessária a gestão do risco dos ativos cujo valor de risco intrínseco seja superior a esse valor.

O limite de risco, ou Risco Aceitável, resulta do equilíbrio entre as medidas de Segurança de Informação a implementar e o impacto dessas. Se não se puderem cumprir essas medidas de segurança, deve-se, ou modificar de novo o limite de Risco Aceitável pela Gestão de Topo, ou, aplicar novas medidas de Segurança de Informação. Será uma decisão da Gestão de Topo da organização!

O limite de risco do serviço é definido e revisto num determinado período temporal e aprovado diretamente pela Gestão de Topo, mesmo que se mantenha o nível do período anterior. Para aqueles riscos que ultrapassam o limite de risco aceitável, realiza-se um procedimento de Tratamento de Riscos.

Respondendo claramente à **questão 2)** do ponto 4. do capítulo I “Qual o método a usar na aplicação do Modelo ao Caso de Estudo?” Face ao desenvolvimento do presente capítulo V, o **método** *utilizado foi o do cálculo do risco intrínseco através da integração de um modelo de gestão de risco integrado com as normas ISO27005 e ISO31000, que se descreve infra.*

CAPÍTULO VI - Resultados

Validação dos Resultados

Através da aplicação do modelo integrado de gestão de risco de Segurança de Informação, pelas normas ISO31000 e ISO27005, foi possível aplicar técnicas de medida do risco intrínseco, das quais se apuraram os seguintes resultados:

- ✓ Entre janeiro de 2019 e julho de 2020 foram identificados 973 incidentes de Segurança de Informação na ANSR. (Tabela 3);

- ✓ Por uma questão de coerência de resultados optou-se pelo foco da análise dos dados para a investigação, apenas no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020, verificando que só foi possível recolher dados até julho de 2020;

- ✓ Neste seguimento, para o período homólogo janeiro a julho de 2019 e 2020, foram apurados 728 incidentes de Segurança de Informação na ANSR. (Tabela 4);

- ✓ Dos 728 incidentes de segurança apurados no período homólogo, 178 foram verificados em 2019 e 550 em 2020 (Tabela 4);

- ✓ Entre janeiro de 2019 e julho de 2020 foram identificados 178 ativos da ANSR (Tabela 8);

- ✓ Destes 178 ativos foi efetuada a agregação dos mesmos por classes de ativos (Tabela 12):

    - ATIVO I PRESIDÊNCIA ANSR;
    - ATIVO II DIRIGENTE ANSR;
    - ATIVO III TÉCNICO ANSR.

- ✓ Da análise de impacto realizada a esses ativos, através da aplicação de matrizes de impacto e de ponderação do impacto sobre os 178 ativos da ANSR (Tabela 13 e Tabela 14), no período homólogo, foram identificados, no ponto 5.1. do Capitulo V, os seguintes valores de impacto sobre os ativos:

    - ATIVO I Valor de impacto 5;
    - ATIVO II Valor de impacto 5;
    - ATIVO III Valor de impacto 4.

- ✓ Da escala de identificação das ameaças (ponto 5.2.1. do Capítulo V) foram apurados os seguintes valores de ameaças:

- **Antes da Pandemia janeiro 2019 a julho 2019 (178 eventos num período de 7 meses)**
  - Ameaça Baixa.

- **No decorrer da Pandemia janeiro 2020 a julho 2020 (550 eventos num período de 7 meses)**
  - Ameaça Alta.

✓ No caso das vulnerabilidades, foi identificada a principal vulnerabilidade relacionada com a condição de teletrabalho: Trabalho não supervisionado por perfis de responsabilidade da organização;

✓ Dos 178 ativos do âmbito identificado no ponto 4. do Capitulo V (Figura 22) no período homólogo, tendo em conta a escala de identificação das vulnerabilidades (ponto 5.2.2. do Capitulo V) foram apurados os seguintes valores de vulnerabilidades:

- **Antes da Pandemia janeiro 2019 a julho 2019 (estavam 23 ativos em teletrabalho)**
  - 12,92% dos ativos Vulnerabilidade Baixa

- **No decorrer da Pandemia janeiro 2020 a julho 2020 (178 ativos em teletrabalho)**
  - 100% dos ativos Vulnerabilidade Alta

✓ Para o valor das ameaças e vulnerabilidades identificados, para cada período homólogo, foi apurado o risco intrínseco para cada classe de ativos do âmbito (ponto 5.3.1. do Capítulo V) em que:

- **Antes da Pandemia janeiro 2019 a julho 2019 (**Tabela 18**)**
  - RAtivoI Risco Intrínseco do Ativo I = 5
  - RAtivoI Risco Intrínseco do Ativo II = 5
  - RAtivoI Risco Intrínseco do Ativo III = 4
  - Risco Total Intrínseco dos Ativos em teletrabalho em 2019 (5) na escala definida é considerado **Medio Risco**.

- **Depois da Pandemia janeiro 2020 a julho 2020 (**Tabela 19**)**
  - RAtivoI Risco Intrínseco do Ativo I = 7
  - RAtivoI Risco Intrínseco do Ativo II = 7
  - RAtivoI Risco Intrínseco do Ativo III = 6
  - Risco Total Intrínseco dos Ativos em teletrabalho em 2019 (7) na escala definida é considerado **Alto Risco**.

Podemos assim observar os valores resumo para o período homólogo analisado, na Tabela 20:

Tabela 20 – Valores resumo no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020

ANTES DA PANDEMIA JANEIRO DE 2019 A JULHO 2019	DEPOIS DA PANDEMIA JANEIRO DE 2020 A JULHO DE 2020	Δ PERIODO HOMÓLOGO
% de Ativos em Teletrabalho		
12,92%	**100%**	Houve um aumento de 87,08% de ativos colocados em teletrabalho.
% de eventos de incidentes de segurança verificados		
24,45%	**75,55%**	Os eventos de incidentes de segurança aumentaram em 51,1%.
Valor Risco Intrínseco Apurado		
Médio Risco = 5	**Alto Risco = 7**	Aumentou em 2 valores passando de Médio Risco para Alto Risco.

Respondendo claramente à **questão 3)** do capítulo I "Como apurar o valor risco para a Segurança de Informação das organizações?" Face à validação de resultados do presente Capitulo VI, é possível apurar o valor do risco intrínseco aplicando as métricas e metodologias de um modelo de gestão de risco integrado com as normas ISO27005, ISO31000, através da adaptação do Anexo C ao Anexo E da ISO27005 às fases do modelo de gestão de risco da ISO31000 [35], [40].

Pelos dados recolhidos na Tabela 20 valida-se a **hipótese** formulada no Capitulo V, ou seja, o modelo proposto na presente dissertação, de gestão de risco de Segurança de Informação permite apurar o risco intrínseco das vulnerabilidades e ameaças, dos ativos da ANSR, em contexto de teletrabalho, i.e., apurou-se o risco de nível **ALTO** com valor 7, para os ativos da ANSR adaptados a novas formas de organização do trabalho, tornando assim possível a ***avaliação e monitorização do risco de Segurança de Informação, no contexto das novas formas de organização do trabalho***.

CAPÍTULO VII - Conclusões

Conclusões

No final de 2019, o mundo deparou-se com uma pandemia, a COVID-19. Em dezembro de 2019 registou-se o primeiro caso em Wuhan, China, poucos meses mais tarde, a 11 de março de 2020, a organização Mundial de Saúde (OMS) declarou a pandemia global [11]. Este estado de pandemia, veio potenciar todas as vulnerabilidades supra identificadas, i.e., veio aumentar os níveis de stress, ansiedade, depressão, não só pela situação de medo vivida, mas também pela alteração de circunstâncias laborais, como a utilização do regime de teletrabalho quase a 100% em determinadas organizações.

Num estudo recente (maio/2020), da Universidade de Coimbra, em colaboração com outras universidades internacionais, é demonstrado o impacto psicossocial da COVID-19 em Portugal, nas duas fases de confinamento COVID19, nas quais a maior parte das organizações optaram por colocar os seus colaboradores em teletrabalho. Foi evidenciado o crescimento de fatores de ansiedade, stress e depressão. O confinamento à habitação, e consequente isolamento social, gerou impactos ao nível da indiferenciação entre o local de lazer e o local de trabalho (teletrabalho), o que, entre outros aspetos, gerou uma situação de grande stresse refletindo-se socialmente em grande parte da população ativa [50].

Numa perspetiva do bem-estar individual dos participantes do estudo realizado, uma grande parte destes revelaram estar extremamente preocupados com a pandemia de COVID-19, destes, todos se encontravam a desempenhar as suas funções laborais em teletrabalho. Da análise feita aos resultados obtidos no estudo realizado, relativamente ao stresse, ansiedade e depressão, causados pela pandemia, pode ser observada a evolução dos mesmos na Figura 23, onde é possível verificar que os valores (severidade dos sintomas) Normal e Leve diminuem durante o isolamento social, e os valores Moderada, Severa e Extremamente Severa aumentam durante o período de isolamento social [50].

	Percentagens antes do isolamento social*			Percentagens durante o isolamento social**		
	Stresse	*Ansiedade*	*Depressão*	*Stresse*	*Ansiedade*	*Depressão*
(Severidade sintomas)						
Normal	77.5	40.8	62.4	73.6	41.3	62.1
Leve	16.6	35.4	25.1	14.9	30.5	23.6
Moderada	4	17.9	11.1	10.4	20.9	12.2
Severa	0.6	4.3	1.3	1.1	5.9	1.5
Extrem. severa	0	1.4	0.2	0	1.4	0.5

*Antes do dia 18 de março
** Depois do dia 18 de março

Figura 23 – Evolução de Severidades de Sintomas Stress, Ansiedade e Depressão antes e após isolamento social derivado da pandemia COVID-19 Fonte: [50]

Conjugando o estudo da Dr.ª Mónica Whitty com estudo realizado pela Universidade de Coimbra, existe algo que os associa, pese embora o primeiro tenha sido efetuado num contexto sem pandemia mundial e sem se suspeitar que esta realidade viesse a acontecer. Ainda assim, constata-se que algo os relaciona, como, por exemplo, o facto de o impacto psicossocial de condições externas às organizações poder influenciar o fator humano intrínseco às mesmas, como são os seus colaboradores [26], [50]. O CNCS entidade articulada com o CCD, refere um possível aumento de incidentes de Segurança de Informação (*phishing*), relacionados com o estado pandémico atual e o isolamento de pessoas em trabalho à distância, no entanto, o Relatório Cibersegurança em Portugal – Sociedade, do Observatório de Cibersegurança, publicado em dezembro do corrente ano, por esta entidade, apenas evidencia indicadores de dados de 2019, alegando que não é assim possível identificar consequências da pandemia Covid-19 [10]. Não obstante as conclusões do Relatório do CNCS, foram várias as entidades nacionais e internacionais, que constataram a relação da pandemia Covid-19 e as novas formas de trabalho, com o aumento de eventos de incidentes de segurança, tais como *ENISA*, *Ernst & Young*, *Infosecurity Magazine*, entre outras.

A presente dissertação pretendeu contribuir para enfatizar essas constatações, propondo ainda um modelo de gestão de risco que permitisse apurar o risco intrínseco de ativos em teletrabalho, ou seja, o risco de determinados ativos sem controlos de segurança adequados à realidade atual de novas formas de trabalho. Desta forma colocou-se a questão principal no capítulo I:

Como avaliar e monitorizar o risco para a Segurança de Informação das novas formas de organização do trabalho?

No decorrer da dissertação fomos recolhendo respostas às questões secundárias que de certa forma vão contribuir para a resposta à pergunta principal, as quais se representam na Tabela 21 nomeadamente:

Tabela 21 – Valores resumo no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020

QUESTÃO SECUNDÁRIA	RESPOSTA	DEMONSTRAÇÃO
questão 1) do ponto 4. do capítulo I: Qual o modelo adequado para avaliar e monitorizar o risco para a Segurança de Informação?	*O modelo adequado para avaliar e monitorizar o risco para a Segurança de Informação é o modelo ISO.*	Capítulo II
questão 2) do ponto 4. do capítulo I: Qual o método a usar na aplicação do Modelo ao Caso de Estudo?	*O método utilizado foi o do cálculo do risco intrínseco através da integração de um modelo de gestão de risco integrado com as normas ISO27005, ISO31000.*	Capítulo III
questão 3) do ponto 4 do capítulo I: Como apurar o valor risco para a Segurança de Informação das organizações?	*É possível apurar o valor do risco intrínseco aplicando as métricas e metodologias de um modelo de gestão de risco integrado com as normas ISO27005, ISO31000, através da adaptação dos Anexo C ao Anexo E da ISO27005 às fases do modelo de gestão de risco da ISO31000.*	Capítulo V

Com base na recolha de respostas às questões secundárias (Tabela 21) e às desmonstrações das mesmas que percorreram os capítulos da presente dissertação, podemos concluir a resposta à pergunta principal formulada:

> ***Como avaliar e monitorizar o risco para a Segurança de Informação das novas formas de organização do trabalho?***
>
> **Resposta:** A avaliação do risco para a Segurança de Informação das novas formas de organização do trabalho, pode ser promovida pela adoção de um modelo de gestão de risco de Segurança de Informação, integrado pelas normas ISO31000 e ISO27005, com os contributos de outras normas ISO identificadas na Tabela 2, identificando: o âmbito de aplicação do modelo de gestão de risco, os ativos e a valorização de impacto, as vulnerabilidades e ameaças a esses ativos e, consequentemente, o apuramento do risco intrínseco do mesmo.

A motivação da presente dissertação, conforme indicado no Capitulo I, tem como pressuposto, acompanhar as conclusões de várias entidades, nacionais e internacionais, no domínio da Segurança de Informação, em contexto pandemia Covid-19, através do Caso de Estudo caracterizado no Capitulo III, foi assim possível através do modelo de gestão de risco adotado e do risco intrínseco apurado, relacionar diretamente o teletrabalho em contexto pandemia Covid-19, com o aumento de eventos de ameaças de Segurança de Informação às organizações.

Foi possível relacionar, o aumento significativo dos ataques evidenciados nas Tabela 7 e Figura 20, com o facto, de no decorrer do inicio de 2020 os colaboradores da ANSR, terem sido quase na sua totalidade colocados em regime de teletrabalho e, face às condicionantes de isolamento social, terem sido "alvos" mais fáceis por técnicas de Engenharia Social, com as mais variadas motivações, agindo por simples negligência, ou por fatores psicossociais (stresse, ansiedade, depressão) que os tenham levado a reduzir o cuidado e segurança na utilização dos meios e ferramentas de trabalho, em regime de teletrabalho.

Todo este cenário revelou a importância de ser aplicado um modelo de gestão de risco de Segurança de Informação na ANSR, face às vulnerabilidades psicossociais, dos seus colaboradores, em contexto de teletrabalho e isolamento social, potenciarem o aumento de probabilidade de concretização de ataques via Engenharia Social, e como consequência acesso e manipulação (alteração, deterioração, eliminação, divulgação, etc…) à informação classificada da ANSR, por pessoas não autorizadas com intenções maliciosas.

Assim, acompanhado os estudos das entidades nacionais e internacionais, sobre o impacto do Covid-19 no aumento de ameaças, face à conjuntura atual de teletrabalho, respondendo claramente à hipótese formulada para o problema identificados no ponto 1. do Capítulo V:

- O **problema identificado** foi: o aumento de eventos de incidentes de segurança, entre janeiro de 2019 e julho de 2010. Especificamente no período homólogo janeiro a julho de 2019 e janeiro a julho de 2020.

- A **hipótese formulada** foi: estará o aumento de eventos de segurança, no período homólogo evidenciado no problema identificado, relacionado com a colocação massiva de colaboradores da ANSR em teletrabalho derivado do contexto pandémico Covid-19?

- **Validação da hipótese**: Houve de facto um aumento do risco intrínseco de 2019 para 2020, no período homólogo analisado, de Médio Risco para Alto Risco, aliado a este facto concluiu-se também pela análise de dados no ponto 3. do Capitulo V, que conforme representado na Figura 19 e Tabela 7 foi observado que em 2019 a maior ocorrência de incidentes de Segurança de Informação (cerca de 82%) ocorreu dentro do período laboral (9:00 às 18:00), já em 2020 a ocorrência desses incidentes dá-se de uma forma quase equilibrada dentro e fora do período laboral, ou seja, 49,64% dentro do período laboral e 50,36% fora do horário laboral.

Trabalho Futuro

Numa perspetiva futura, seria interessante que se pudessem avaliar fatores psicossociais dos colaboradores das organizações, inserido em contexto de medicina do trabalho, numa previsão de análise de risco dos mesmos. Trata-se de uma situação delicada, ao verificar que podem estar em causa questões de privacidade dos mesmos. No entanto as organizações podem promover encriptação dos dados recolhidos para avaliação de risco ou promover a anonimização e pseudonimização os mesmos.

A proposta para o futuro seria promover um modelo conjunto entre o demonstrado na presente dissertação e o modelo apresentado para prevenir *insider threats* pela Dr.ª Monica Whitty [26].

REFERÊNCIAS

Para a referência bibliográfica, a autora do relatório utiliza a norma (IEEE) Institute of Electrical and Electronics Engineers[1]. A respetiva referência bibliográfica, consta de uma lista no final do relatório, organizada numericamente, apresentando entre parênteses retos, o número da citação de acordo com a ordem em que aparecem no relatório.

[1] P. F. Drucker, *Inovação e Gestão*, 4ª Edição. Lisboa, 1997.

[2] L. A. I. V. dos Santos and M. R. M. Marques, "Cyberlaw by CIJIC, Direito: a pensar tecnologicamente," vol. EDIÇÃO N.º, no. Gestão de Risco Aplicada à Segurança de Informação, p. 37, May 2019.

[3] L. V. dos Santos, "O Controlo do Funcionamento das Instituições Democráticas num Contexto de Ciberespaço," 2019.

[4] Instituto da Defesa Nacional, "Revista Quadrimestral - idn nação e defesa n.º 133," *Revista Quadrimestral - idn nação e defesa - n.º 133*, vol. 133, no. Cibersegurança, p. 266.

[5] I. Magazine, "COVID19 Aumenta 667% de e-mails de phishing em menos de um mês," *26 de março 2020*, 2020.

[6] S. M. – A. P. EY, "Webinar APDC: Cibersegurança no contexto do Teletrabalho," 2020. [Online]. Available: https://static.viatecla.com/apdc/share/2020-04/2020-04-22145047_f7664ca7-3a1a-4b25-9f46-2056eef44c33$$72F445D4-8E31-416A-BD01-D7B980134D0F$$DB66862F-9EC4-42FC-835D-4CD1BFF271C9$$storage_image$$pt$$1.pdf. [Accessed: 22-Apr-2020].

[7] J. Publico, "Covid-19: Centro Nacional de Cibersegurança identifica 71 casos de phishing até Abril," *Covid-19: Centro Nacional de Cibersegurança identifica 71 casos de phishing até Abril*, 2020. [Online]. Available: https://www.publico.pt/2020/04/17/sociedade/noticia/covid19-centro-nacional-ciberseguranca-identifica-71-casos-phishing-ate-abril-1912692. [Accessed: 17-Apr-2020].

[8] J. Publico, "O que diz o decreto sobre o estado de emergência: ponto a ponto," *Publico, Jornal*, 2020. [Online]. Available: https://www.publico.pt/2020/03/18/politica/noticia/decreto-estado-emergencia-ponto-ponto-1908412. [Accessed: 18-Mar-2020].

[9] ENISA, "Compreendendo e lidando com phishing durante a pandemia COVID-19." [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic.

[10] C. N. de C. CNCS, "Cibersegurança em portugal," Lisboa, 2020.

[11] Serviço Nacional de Saúde, "COVID-19," 2020. [Online]. Available: https://www.sns24.gov.pt/tema/doencas-infecciosas/covid-19/#sec-0.

[12] D. da R. Eletrónico, "Código do Trabalho Lei n.º 7/2009," 2009. [Online]. Available: https://dre.pt/legislacao-consolidada/-/lc/75194475/201707240900/73439934/diploma/indice.

[13] R. Ritmos, "Recebeu um email (falso) Seg. Rodoviária? É Fraude," 2020. [Online]. Available: https://www.radioritmos.com/recebeu-um-email/. [Accessed: 22-Jul-2020].

[14] P. Sapo, "Atenção à mensagem para pagar uma contraordenação! É Phishing…," 2020. [Online]. Available: https://pplware.sapo.pt/informacao/atencao-a-mensagem-para-pagar-uma-contraordenacao-e-phishing/. [Accessed: 25-Nov-2020].

1 (IEEE) referência bibliográfica, vocacionada para as áreas de Engenharia (concretamente: computação, eletrónica, energias, robótica e tecnologias aplicadas).

[15] T. Sintra, “GNR ALERTA PARA FRAUDE POR EMAILS EM NOME DA AUTORIDADE NACIONAL DE SEGURANÇA RODOVIÁRIA,” 2020. [Online]. Available: https://tvsintra.wordpress.com/2020/12/16/gnr-alerta-para-fraude-por-emails-em-nome-da-autoridade-nacional-de-seguranca-rodoviaria/. [Accessed: 16-Dec-2020].

[16] C. P. Coutinho, *Metodologia de Investigação em Ciências Sociais e Humanas Teoria e Prática*, 2ª. Coimbra: Grupo Almedina, 2015.

[17] P. E. e do C. J. O. D. U. Europeia., *Diretiva UE 2016/1148. Segurança das redes e da informação em toda a União Europeia, do Parlamento Europeu e do Conselho. Jornal Oficial Da União Europeia.* 2016.

[18] D. da R. Eletrónico, *Regulamento Nacional de Interoperabilidade Digital, Republica, D. da. (2018). Resolução do Conselho de Ministros N. 2 de 2018 (RNID). Diário Da Repúbilica, 1.a Série - N. 4 - 5 de janeiro de 2018.*, Resolução. 2018.

[19] P. E. e Conselho, “Regulamento UE 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016,” *J. Of. da União Eur.*, p. 88, 2016.

[20] and L. S. A. P. Relvas, A. Portugal, S. Major, “Preliminary Results on the Psychosocial Impact of COVID-19 in Portugal (in Portuguese),” 2020.

[21] E. A. Holmes *et al.*, “Multidisciplinary research priorities for the COVID-19 pandemic: a call for action for mental health science,” *The Lancet Psychiatry*, vol. 7, no. 6, pp. 547–560, 2020.

[22] A. M. Rea-Guaman, J. Mejía, T. San Feliu, and J. A. Calvo-Manzano, “AVARCIBER: a framework for assessing cybersecurity risks,” *Cluster Comput.*, vol. 23, no. 3, pp. 1827–1843, 2020.

[23] R. S. Dalal, D. J. Howard, R. J. Bennett, C. Posey, S. J. Zaccaro, and B. J. Brummel, “Organizational science and cybersecurity: abundant opportunities for research at the interface,” *J. Bus. Psychol.*, 2021.

[24] J. Guarezi, “Engenharia Social: Avaliação de Riscos e Vulnerabilidades Tendo o Fator Humano como o Elo mais Fraco da Segurança da Informação,” 2019.

[25] T. Grassegger and D. Nedbal, “The role of employees’ information security awareness on the intention to resist social engineering,” *Procedia Comput. Sci.*, vol. 181, no. 2019, pp. 59–66, 2021.

[26] M. T. Whitty, “Developing a conceptual model for insider threat,” *J. Manag. Organ.*, no. 2018, 2018.

[27] C. N. de C. CNCS, “Cibersegurança em portugal - Riscos e Conflitos 2021,” 2021.

[28] M. H. Gallacher Liz, *Liz Gallacher, Helen Morris-ITIL Foundation Exam Study Guide-Sybex (2012)*. 2012.

[29] COBIT 5, Isaca, and C. 5, *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT- Executive Summary*. 2016.

[30] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, “NP ISO 27001:2013 - Tecnoologia de informação Técnicas de segurança Sistemas de gestão de segurança da informação – Requisitos.” p. 32, 2013.

[31] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, “ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.” p. 90, 2013.

[32] IPQ, “NP ISO 31000: Gestão do Risco - Principios e Linhas de Orientação,” 2012.

[33] “ISO / IEC 38500:2015 Information technology — Governance of IT for the organization,” vol. 2015. 2015.

[34] I. Portugal, “ITIL O QUE É,” 2020. .

[35] ISO/IEC, “] ISO/IEC 31000:2018 - Risk Management - Principles and guidelines,” 2018.

[36] ISO/IEC, “ISO/IEC 20000-1: 2018 - Information technology - Service management - Part 1: Service management systems requirements,” 2018.

[37] ISO/IEC, “ISO/IEC 20000-2: 2019 - Information technology - Service management - Part 2: Guidance on application of service management systems,” 2019.

[38] ISO/IEC, “ISO/IEC 20000-3: 2019 - Information technology - Service management - Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1,” 2019.

[39] ISO/IEC, “ISO/IEC 27002:2013 - Tecnologia de informação Técnicas de segurança – Código de boas praticas para Controlos de Segurança da informação.,” 2013.

[40] ISO/IEC, “ISO/IEC 27005: 2018 - Information technology — Security techniques — Information security risk management,” 2018.

[41] ISO/IEC, “ISO/IEC 27032: 2012 - Information technology — Security techniques — Guidelines for cybersecurity,” 2012.

[42] ISO/IEC, “ISO/IEC 31010:2019 - Risk Management – Risk assessement techniques,” 2019.

[43] ISO/IEC, “ISO/IEC 27001:2013 - Tecnologia de informação Técnicas de segurança Sistemas de gestão de segurança da informação – Requisitos,” 2013.

[44] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, “ISO/IEC 31000:2018 - Gestão do Risco e Linhas de Orientação.” 2018.

[45] ISO, “ISO,” 2020. [Online]. Available: https://www.iso.org.

[46] C. D. B. Batista and J. B. R. B. Farinha, “As Variáveis Determinantes Na Escolha Do Modelo De Corporate Governance Em Portugal,” pp. 1–67, 2009.

[47] IPAC, “BASE DE DADOS NACIONAL SISTEMAS DE GESTÃO CERTIFICADOS,” 2020. [Online]. Available: http://www.ipac.pt/pesquisa/pesq_empcertif.asp.

[48] ANSR, “A ANSR,” 2020. [Online]. Available: http://www.ansr.pt/AANSR/Pages/default.aspx.

[49] R. Gaspar *et al.*, “Decreto Regulamentar n.º 28/2012 - MAI - Aprova a orgânica da Autoridade Nacional de Segurança Rodoviária,” *Diário da República N.º 51 — 12 março 2012*, vol. 1.ª série, pp. 1091–1093, 2012.

[50] A. P. Relvas, A. Portugal, S. Major, and L. Sotero, “Resultados Preliminares sobre Impacto Psicossocial da COVID-19 em Portugal,” 2020.

[51] OWASP, “Injeção SQL,” 2020. [Online]. Available: https://owasp.org/www-community/attacks/SQL_Injection.

[52] OWASP, “Cross Site Scripting (XSS),” 2020. [Online]. Available: https://owasp.org/www-community/attacks/xss/.

ANEXOS

ANEXO A - CONCEITOS

Para o correto enquadramento da presente dissertação, importa apurar os seguintes conceitos, no âmbito da Segurança de InformaçãoSegurança de Informação:

Ativo - Todo o elemento com valor para a organização e que requer proteção. **[12]** *ISO27005:2018*

Informação - Ativo, tangível ou inatingível, que tem valor para a organização e requer uma proteção adequada **[7]** ISO27001:2013.

Sistema de Informação - Infraestrutura Tecnológica que recorre a hardware e software para tratamento de informação.

Segurança de Informação - Conjunto de medidas técnicas, organizativas/gestão e legais, aplicadas à informação, em qualquer tipo de suporte, mantidas durante todo o ciclo de vida da informação na organização, revistas, medidas e melhoradas **[7]** ISO27001:2013.

Princípios e Objetivos da Segurança de Informação - A Segurança de Informação, pelo standard da ISO27001:2013 rege-se pelos seguintes princípios **[3]**:

- **Confidencialidade** - assegurar que apenas quem está autorizado é que pode aceder à informação.
- **Integridade** - assegurar que a informação e os seus métodos são completos. Isto significa que independentemente dos canais e formas onde a informação possa ser tratada e divulgada, a mesma, nunca perde o seu valor conceptual nem é adulterada.
- **Disponibilidade** - assegurar que os utilizadores autorizados têm acesso à informação e aos seus ativos associados sempre que necessitem.
- **Autenticidade e não repúdio/desconhecimento** - assegurar a fiabilidade das transações e o intercâmbio de informação entre organizações e colaboradores.
- **Legitimidade** - garantir que o tratamento da informação cumpre com as leis e regulamento do sector (área de negócio) a que se aplica.

Destacam-se também os seguintes princípios adicionais às características fundamentais da Segurança de InformaçãoSegurança de Informação:

- A **proteção dos dados** de carácter pessoal e a privacidade das pessoas;
- A **proteção dos direitos** de propriedade intelectual e industrial;
- O estabelecimento de um **sistema de classificação da informação** com o objetivo de proteger melhor os ativos críticos da organização;
- A **salvaguarda** dos registos da organização.

Classificação da Informação - Procedimento interno da organização, de modo a estabelecer níveis de classificação da informação tais como: confidencial, secreta, publica, interna, ou, outro tipo de informação, definindo por cada tipo de classificação de informação, quem pode aceder e, de que modo pode aceder ou divulgar informação. Para além desta definição, deve ainda ser implementado o controlo de versões de informação que possa ser produzida sobre a mesma origem, identificando todas as versões que foram produzidas sobre a mesma informação, datas e autores de versões produzidas,

bem como, identificação de que informação adicional acrescida, ou, que informação foi retirada da inicial. **[3]**

Sistema de Gestão de Serviços TI (SGSTI) - Modelo de gestão implementado numa organização, para gestão de serviços de Tecnologias de Informação.

Sistema de Gestão de Segurança de Informação (SGSI) - Modelo de gestão implementado numa organização, para gestão de Segurança de Informação.

Risco - Efeito de incerteza nos objetivos, i.e., desvio relativamente ao esperado. Pode ser positivo, negativo ou ambos e pode abordar, criar ou resultar em oportunidades e ameaças. **[5]** ISO31000:2018

Ameaça - Fator com origem interna ou externa à organização, que pode afetar adversamente os seus ativos. As ameaças podem ter origem natural ou humana e podem ser acidentais ou deliberadas. **[12]** ISO27005:2018

Insider Threat - Designação dada em contexto de Cibersegurança de ameaças internas (colaboradores de uma organização), normalmente relacionadas com vulnerabilidades de pessoas.

Vulnerabilidade - Ponto fraco de um ativo ou controlo que pode ser explorado, intencionalmente ou não, por uma ameaça **[13]** ISO27032:2012.

Controlo de Segurança - Medida que mantém e/ou modifica o risco, de forma preventiva ou corretiva **[5]** ISO31000:2018.

Engenharia Social - Táticas de engenharia psicológica ou social, a que recorrem cibercriminosos para terem sucesso nos seus ataques, através de acesso a informações de identificação pessoal ou relacionadas com propriedade intelectual da organização **[13]** ISO27032:2012.

Modelo de Gestão de Risco de Segurança de Informação - Modelo que permite avaliar todas as condicionantes internas e externas, que possam representar riscos significativos para os objetivos (ponto 3.4) da Segurança de Informação de determinada organização, obtendo a análise de impacto dos riscos identificados, antecipando ações preventivas e corretivas a esses, bem como, definir as linhas estratégicas da organização relativamente a este âmbito. Assim, no âmbito da presente dissertação, colaboradores da ANSR em contexto de teletrabalho, iremos focar o modelo de gestão de risco de Segurança de Informação a adotar, de acordo com a Figura 24, ou seja, um modelo que pretende identificar o risco a que estão sujeitos os Objetivos de Segurança de Informação, relativos às ameaças e vulnerabilidades implícitas aos ativos dos colaboradores e informação classificada da ANSR.

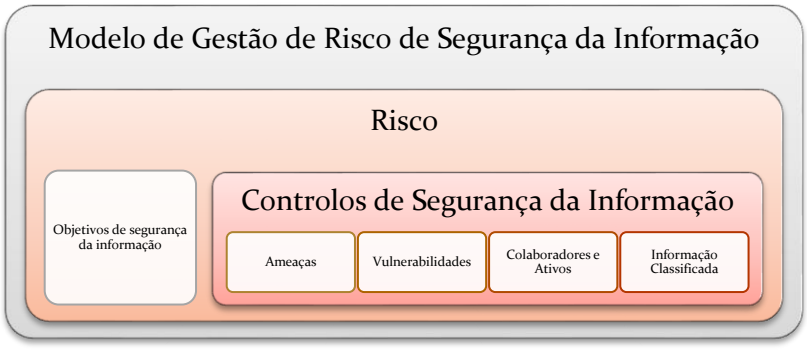

Figura 24 – Modelo de Gestão de Risco de Segurança de Informação que se pretende atingir na presente Dissertação

Malware - software desenhado com intenção maliciosa, contendo recursos ou capacidades que podem potencialmente causar danos direta ou indiretamente ao utilizador, ou ao sistema operativo do equipamento do utilizador [41].

SQL Injection,- técnica que consiste na inserção de consultas SQL (linguagem de programação) através de credenciais ou outros dados de acesso a determinada página (aplicação) web. Este tipo de ataque, se bem-sucedido, pode devolver ou modificar dados confidenciais de determinada base de dados aplicacional, entre outras consequências [51].

JavaScript Injection (Cross-Site Scripting XSS) - técnica que consiste na inserção de scripts (instruções de código) maliciosos em sites confiáveis, permitindo ao atacante aceder a ficheiros temporários de credenciais (cookies de sessão nesse site) ou outras informações confidenciais retidas pelo browser (navegador web) e usadas com aquele site [52].

Phishing - Processo fraudulento de tentativa de adquirir informações privadas ou confidenciais, mascarando-se como uma confiável entidade, via comunicação eletrônica [41].

APÊNDICES

Apêndice 1 – Recolha e ajustamento dos dados Eventos Segurança

CAMPO ORIGINAL	DESCRIÇÃO	ADAPTAÇÃO PARA ANÁLISE DE DADOS	DESCRIÇÃO
Id	id de Ticket	id DO EVENTO	Número de registo do evento utilizado para contabilizar eventos.
Subject	Título do Ticket	ASSUNTO	Utilizado para normalizar os campos TIPO ATAQUE e PONTO DE ENTRADA ATAQUE.
Status	Estado do Ticket	IGNORADO	À data de análise dos dados todos os eventos estavam resolvidos não foi possível analisar histórico de estados.
QueueName	Incidente ou Incidente Response	IGNORADO	Sem dados suficientes para análise. Foram classificados como incidentes todos os eventos pelo campo TIPO ATAQUE.
Criado	Data Criação do Ticket	IGNORADO	O campo não tinha formatação data foi desdobrado em Mês e Ano.
CAMPO ADAPTADO		MÊS	Mês de Criação.
CAMPO ADAPTADO		ANO	Ano de Criação.
CAMPO ADAPTADO		PERIODO DIA	Foi adaptado em função do campo Criação (data de criação do ticket), de modo a perceber a ocorrência de eventos dentro e fora do período laboral (9:00 às 18:00).
CustomField.{Description}	Descrição do Ticket (Caso exista)	DESCRIÇÃO	Utilizado para normalizar os campos TIPO ATAQUE e PONTO DE ENTRADA ATAQUE.
CustomField.{Malware}	tipo de *Malware* associado ao ticket (Caso exista)	TIPO ATAQUE	Foi normalizado em função do campo DESCRIÇÃO e ASSUNTO.
CAMPO ADAPTADO		PONTO ENTRADA ATAQUE	Foi normalizado em função do campo DESCRIÇÃO e ASSUNTO.
CustomField.{Customer}	Entidade (organização do MAI)	ENTIDADE	ANSR.
CustomField.{IP}	IP's associados ao Ticket foi ignorado	IGNORADO	Sem dados suficientes para análise.
CustomField.{IR Resolution}	Tipo de resolução do Ticket (Por exemplo: Falso Positivo, Incidente, Incidente Já Reportado, Mitigado Automaticamente, etc)	IGNORADO	Sem dados suficientes para análise.
CustomField.{TargetHostname}	*Hostname* associado ao Ticket (pode ser Máquinas ou Domínios)	IGNORADO	Sem dados suficientes para análise.
CustomField.{TargetUsername}	*UserName* associado ao ticket (Utilizadores dentro da rede)	IGNORADO	Não foi referenciado por questões de privacidade.

CAMPO ORIGINAL	DESCRIÇÃO	ADAPTAÇÃO PARA ANÁLISE DE DADOS	DESCRIÇÃO
CAMPO ADAPTADO		PERFIL/RESPONSABILIDADE USER	Foi normalizado em função do campo USER ASSOCIADO, por questões de privacidade, estes dados embora tratados não foram representados com a associação dos mesmos aos eventos de ataques identificados também por questões de privacidade.
CustomField.{URL}	URL's contidos no ticket (caso exista)	IGNORADO	Sem dados suficientes para análise.
Parents	Incidente ao qual o Incidente Response esta associado (Caso exista)	IGNORADO	Sem Relevância para a análise.

Apêndice 2 – Recolha e ajustamento dos dados Identificação Ativos

CAMPO ORIGINAL	DESCRIÇÃO	ADAPTAÇÃO PARA ANÁLISE DE DADOS	DESCRIÇÃO
NOME	Identificação do Colaborador ANSR	IGNORADO	Não foi referenciado por questões de privacidade.
RESPONSABILIDADE	Tipo de Perfil do utilizador (Presidência, Dirigente, Técnico)	RESPONSABILIDADE	Utilizado para normalizar o PERFIL do utilizador do ativo.
VINCULO	Tipo de relação contratual do Colaborador (Interno ou Prestador de Serviço)	VINCULO	Utilizado para normalizar o VINCULO do utilizador do ativo.
UNIDADE ORGÂNICA	Unidade Orgânica afeta ao Colaborador	IGNORADO	Utilizado para normalizar o campo UO do utilizador do ativo.
UO	Unidade Orgânica agregadora afeta ao Colaborador	UO	Normalizado em função do campo UNIDADE ORGÂNICA.
AREA	Funções do Colaborador.	AREA	Utilizado para normalizar o campo AREA do utilizador do ativo.
ESTADO VPN/CIRCUITO DIRETO	Acesso aos SI da ANSR pelo Colaborador fora da ANSR (ATIVO/INATIVO)	ESTADO VPN/CIRCUITO DIRETO	Utilizado para normalizar o campo ESTADO VPN/CIRCUITO DIRETO, foram apenas contemplados para a análise os estados ativos.
N.º DO PEDIDO	Campo de controlo interno do NIF	IGNORADO	O campo não foi considerado por ser um controlo operacional de identificação o pedido.