Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

RELATÓRIO DE ESTÁGIO

GESTÃO DE RISCOS DE CIBERSEGURANÇA: GESTÃO DE RISCOS DE CIBERSEGURANÇA DE FORNECEDORES

TAP AIR PORTUGAL

DIOGO ROBERTO LOURENÇO DUARTE

JUNHO - 2023

Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO EM
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
RELATÓRIO DE ESTÁGIO

GESTÃO DE RISCOS DE CIBERSEGURANÇA: GESTÃO DE RISCOS DE CIBERSEGURANÇA DE FORNECEDORES

TAP AIR PORTUGAL

DIOGO ROBERTO LOURENÇO DUARTE

ORIENTAÇÃO:

PROFESSOR DOUTOR SÉRGIO RODRIGUES NUNES

JUNHO - 2023

Agradecimentos

A persistência é o caminho do êxito.

Charles Chaplin

Vida e Pensamentos. Editora Martin Claret. 1997. p. 118

A realização deste relatório é a minha forma de agradecer principalmente aos meus, não só em palavras, mas, como prova de toda a dedicação, esforço e fé na minha persistência e na de todos que acreditaram em mim para conseguir chegar aqui. Foi um caminho atribulado, nem sempre fácil, mas é um objetivo alcançado. O marco de uma nova etapa, o início de projetos e objetivos que irão surgir e, pelos quais irei trabalhar para os alcançar.

Começo assim com um agradecimento especial aos meus pais, pelo amor incondicional e por sempre acreditarem em mim, sendo o seu suporte fundamental para ultrapassar diversos obstáculos durante todo este percurso. Aos meus modelos de coragem, pai e mãe o meu muito obrigado.

Ao meu coordenador de estágio na TAP, António Carrilho, o meu muito obrigado pela resposta ao email que me permitiu ter a experiência incrível na TAP, bem como, toda a aprendizagem que tive ao longo destes 6 meses de estágio.

Ao Prof. Dr. Sérgio Nunes, orientador de estágio pelo apoio e orientação nesta fase e, ao Prof. Dr. Rui Guedes pelo apoio e orientação em decisões importantes que complementaram este meu percurso.

Por último, tendo consciência que sozinho nada disto seria possível, um agradecimento especial à minha namorada, pelo apoio incondicional, incentivo, amor, amizade, paciência e ajuda na superação dos obstáculos ao longo do início desta caminhada até a este momento.

A todos vocês o meu muito obrigado. A eles dedico este trabalho!

Resumo

Cada vez mais as organizações estão sujeitas a uma maior exposição a ciberataques, devido à dinâmica e disrupção que transformam e caracterizam o ciberespaço. O número e diversidade de ciberataques aumenta a cada dia, e os ativos críticos de informação das empresas são cada vez mais valiosos, quer para a própria organização, quer para os cibercriminosos.

A importância da Segurança da Informação e Cibersegurança é cada vez maior devido ao número de tecnologias e soluções disponíveis no mercado, aumentando a superfície de ataque, devendo por isso as empresas ver a *InfoSec* e a Cibersegurança como um investimento, ao invés de um custo.

Atualmente, os fornecedores são uma das principais causas que tornam as empresas vulneráveis a um possível ciberincidente, sendo por isso fundamental implementar e manter processos que garantam a correta Gestão dos Riscos de Cibersegurança de Fornecedores, pelo que as principais atividades realizadas durante o estágio (relacionadas com o desenvolvimento de um *Framework* para a Gestão de Riscos de Cibersegurança de Fornecedores), são cruciais para a TAP, no sentido de evitar possíveis impactos derivados de ciberincidentes de fornecedores, garantindo desta forma a resiliência e a proteção dos princípios de Confidencialidade, Integridade e Disponibilidade, reforçando assim a eficácia e sucesso do seu programa/plano de Segurança da Informação.

Neste sentido, o objetivo principal do estágio consistiu em desenvolver um *Framework* para supervisionar os riscos de Cibersegurança de fornecedores da TAP, que permita avaliar o nível de risco de potenciais riscos dos fornecedores, avaliando tanto a probabilidade da sua ocorrência como o seu potencial impacto. O objetivo final é integrar os resultados deste *Framework* no Programa de Gestão de Riscos de Cibersegurança da TAP.

Abstract

Organizations' exposure to cyber attacks is increasing quickly due to the dynamics and disruption that transform and characterize the cyberspace. The number and diversity of cyber attacks are rising every day, and companies' critical information assets are becoming more valuable, to the organization itself and to cyber criminals.

The importance of Information Security and Cybersecurity is on the rise whereas the number of technologies and solutions available in the market expand companies' attack surface. Therefore, InfoSec and Cybersecurity should be seen as an investment, rather than a cost.

Nowadays, 3rd Parties are one of the main causes that make companies vulnerable to a possible cyber incident, so it is essential to implement and maintain processes that ensure the correct management of 3rd Party Cybersecurity risks. Therefore, the main activities carried out during the internship (related to the development of a 3rd Party Cybersecurity Risk Management Framework) are crucial for TAP, to avoid possible impacts from 3rd Party cyber incidents, thus ensuring the resilience and protection of information Confidentiality, Integrity and Availability, reinforcing the effectiveness and success of its Information Security program/plan.

In this regard, the primary goal of the internship was to develop a framework for overseeing TAP's 3rd Party Cybersecurity Risks. This framework aims to assess the risk level associated with potential supplier risks by evaluating both the likelihood of their occurrence and their potential impact. The ultimate objective is to integrate the outcomes of this framework into TAP's Cybersecurity Risk Management Program.

Índice de acrónimos

C.I.A = Confidentiality, Integrity, Availability = Confidencialidade, Integridade e Disponibilidade

CISA = U.S. Cybersecurity & Infrastructure Security Agency

CISO = Chief Information Security Officer

CNCS = Centro Nacional de Cibersegurança

CNPD = Comissão Nacional de Proteção de Dados

DMZ = Demilitarized Zone = Zona Desmilitarizada

DNS = Domain Name System

FAA = Federal Aviation Administration

IATA = International Air Transport Association

InfoSec = Information Security

IoT = Internet of Things

ISMS = Information Security Management System = Sistema de Gestão de Segurança da Informação

SOC = Security Operations Center

TAP = Transportes Aéreos Portugueses, S.A.

TFM = Trabalho Final de Mestrado

TIC = Tecnologias de Informação e Comunicação

TPCRM = 3rd Party Cybersecurity Risk Management = Gestão de Riscos de Cibersegurança de Fornecedores

Índice

Índice de Figuras

1. Introdução

No âmbito da realização do TFM em Gestão de Sistemas de Informação, no Instituto Superior de Economia e Gestão da Universidade de Lisboa (ISEG), decidi realizar um estágio curricular e o respetivo relatório de estágio.

O estágio foi realizado na empresa TRANSPORTES AÉREOS PORTUGUESES, S.A. (Tap Air Portugal), com uma duração total de 787 horas, entre os dias 3 de outubro de 2022 e 31 de março de 2023, sob orientação académica do Prof. Dr. Sérgio Rodrigues Nunes, e orientação na empresa, do *Deputy* CISO António Carrilho. Após uma entrevista com os responsáveis pelos *Digital & Technlogy Services* da TAP Air Portugal, na qual foi proposta a possibilidade de realizar o estágio no recém-constituído departamento de Cibersegurança (*Cybersecurity Services*), com foco na Gestão de Riscos de Cibersegurança, decidi aceitar esta oportunidade, pela crescente relevância que a Segurança da Informação e Cibersegurança tem ganho nos últimos anos, considerando também o facto que no futuro maior parte das organizações terão necessariamente de investir neste domínio, o que exponencia as oportunidades que daí podem derivar.

De modo a realizar um breve enquadramento, considera-se que a Gestão de Riscos de Cibersegurança está incluída na Cibersegurança e esta por sua vez é um subconjunto da Segurança da Informação. A Segurança da Informação (*InfoSec*) é uma preocupação crescente das diversas organizações, devido à globalidade do mercado em que operam, elevada dependência de TIC, transformação digital, e porque cada vez mais a presença digital das empresas é maior, sendo considerada essencial para o funcionamento das suas operações, e consequentemente, para o sucesso empresarial das organizações (Antunes *et al.*, 2021). Consideráveis quantias são dedicadas à Gestão de Riscos de Cibersegurança, sobretudo porque as indústrias, indivíduos e nações consideram o risco cibernético como extremamente preocupante e capaz de

prejudicar de forma dramática o sucesso das organizações (Paté-Cornell *et al.*, 2018).

As principais atividades realizadas no estágio estão relacionadas com a Gestão de Riscos de Cibersegurança, sendo esta identificada como uma das primeiras linhas de defesa e prevenção da Cibersegurança, permitindo às organizações tomar decisões de forma priorizada e informada com base na análise de vulnerabilidades e ameaças que se poderão traduzir em riscos, e consequentemente em ciberincidentes, podendo provocar graves impactos nas operações, resultados financeiros, *compliance* ou reputação das organizações. A Gestão de Riscos de Cibersegurança de Fornecedores de TIC (de agora em diante denominada por TPCRM) foi o principal foco das atividades do estágio, sendo importante referir que segundo o artigo 21º da Diretiva NIS2, as entidades essenciais e importantes devem implementar medidas técnicas, operacionais e organizativas que permitam gerir os riscos de Cibersegurança, incluindo os riscos da sua cadeia de abastecimento, pelo que a correta implementação da TPCRM é fundamental para garantir *compliance* com os requisitos legais europeus.

O presente relatório está estruturado em 6 capítulos. No 1º capítulo, é realizada uma introdução para contextualizar o estágio realizado. De seguida, no 2º capítulo, é feito um enquadramento teórico, onde se pretende enquadrar e clarificar o que se entende por *InfoSec*, Cibersegurança, Gestão de Riscos de Cibersegurança, TPCRM, bem como endereçar o estado atual da Cibersegurança no sector aeronáutico, com o intuito de facilitar o entendimento das atividades realizadas ao longo do estágio. No 3º capítulo, é realizada uma apresentação da TAP Air Portugal. O 4º capítulo descreve as atividades desenvolvidas durante o estágio. No 5º capítulo é realizada uma reflexão crítica, que consiste num confronto entre a componente teórica (enquadramento teórico) e a componente prática (atividades desenvolvidas no estágio). Por último, o 6º capítulo é composto pelas considerações finais, formuladas com base no conhecimento e experiência obtidos no estágio.

2. Enquadramento Teórico

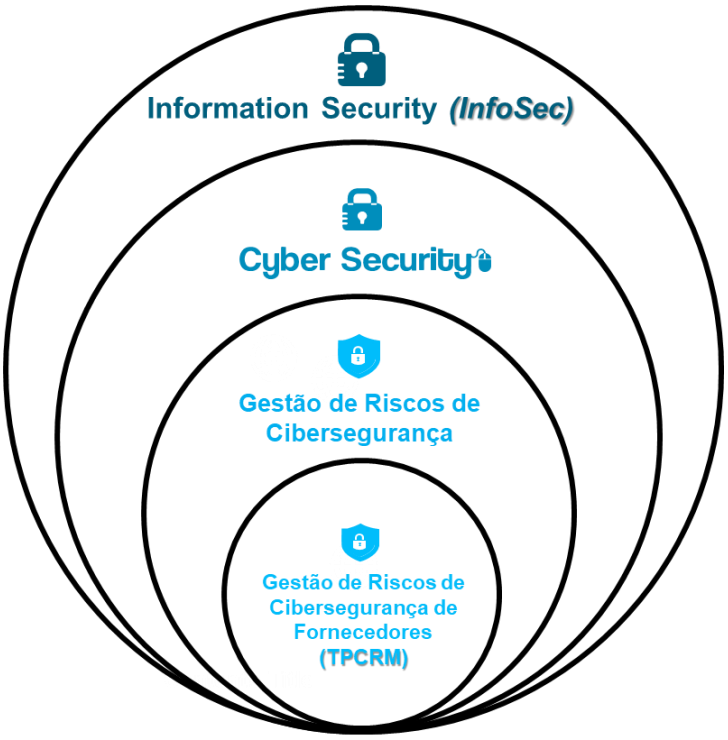


Figura 1 - Estrutura hierárquica dos conceitos fundamentais descritos no Capítulo I. Fonte: elaboração própria

2.1. Segurança da Informação (*InfoSec*)

A *InfoSec* pode ser definida como a preservação/proteção da Confidencialidade, Integridade e Disponibilidade (Tríade C.I.A) da informação (von Solms e von Solms, 2018). É essencial proteger a informação da publicação, cópia, transferência, modificação ou eliminação não autorizada, quer estas ações sejam acidentais ou intencionais. Um dos principais objetivos da *InfoSec* é garantir a continuidade de negócio e minimizar os danos que poderão resultar de possíveis incidentes de Segurança da Informação (von Solms e van Niekerk, 2013).

A informação pode assumir diversas formas, i.e., informação física, informação verbal e informação digital (von Solms e van Niekerk, 2013). Neste sentido, a *InfoSec* deverá garantir a proteção da informação de todos os tipos e em todos os ambientes.

"A *InfoSec* é algo que se faz, não algo que se tem" (van Daalen, 2022, p.1). Segundo a ISO 27002, é alcançada através da implementação de um conjunto de controlos técnicos e organizacionais, políticas, regras, processos, procedimentos, *hardware* e *software*. Para endereçar os objetivos específicos de segurança e de negócio, as organizações devem definir, implementar, monitorizar, rever e melhorar os vários aspetos mencionados anteriormente (International Organization for *Standard*ization, 2022).

A Segurança da Informação desempenha um papel crucial na proteção dos ativos de informação e das operações das organizações. Se for gerida e implementada corretamente, contribui de forma significativa para a reputação e aumento do valor da empresa (AlGhamdi *et al.*, 2020).

Os termos *InfoSec* e Cibersegurança são frequentemente confundidos e usados indistintamente (von Solms e van Niekerk, 2013). A principal diferença entre Cibersegurança e *InfoSec* é que a Cibersegurança apenas tem como âmbito de atuação o ciberespaço (informação digital), enquanto a *InfoSec* tem um âmbito mais geral de atuação, ou seja, a proteção da informação de todos os tipos e em todos os ambientes (B. von Solms e von Solms, 2018).

2.2. Cibersegurança

Várias instituições de renome na área da *InfoSec*, como por exemplo ISO, NIST ou ISACA, consideram que a Cibersegurança é um subconjunto, ou seja, está contida na *InfoSec* (von Solms e von Solms, 2018).

Existem inúmeras definições de Cibersegurança. A Cibersegurança é definida por vários especialistas como sendo um conjunto de tecnologias, processos, práticas, respostas e medidas de mitigação para proteger redes, computadores, programas e dados, de ataques e danos ou de acesso não autorizado, de forma a garantir a Confidencialidade, Integridade e Disponibilidade (Craigen *et al.*, 2014). "A Cibersegurança é a preservação da

Confidencialidade, Integridade e Disponibilidade da informação no ciberespaço" (von Solms e von Solms, 2018, p.5). Cibersegurança traduz-se nas capacidades de garantir a Integridade, Confidencialidade e Disponibilidade dos dados no ciberespaço, tomando as medidas necessárias para prevenir ataques, intrusões, interferências, destruição, uso ilegal e ciberincidentes que possam impactar as operações, resultados financeiros, *compliance* e reputação das organizações (Guo, 2018).

Devido à importância que a Gestão de Riscos de Cibersegurança tem ganho nos últimos anos, a definição de Cibersegurança tem sofrido algumas adaptações e é por alguns definida como sendo a abordagem e as ações associadas com os processos de Gestão de Riscos de Cibersegurança seguidas pelas organizações, com o objetivo de proteger a Confidencialidade, Integridade e Disponibilidade dos dados e dos ativos no ciberespaço (Kianpour *et al.*, 2022).

2.3. Gestão de Riscos de Cibersegurança

Diversos especialistas indicam que os ciberataques poderão ser a maior ameaça a qualquer organização, enquanto uma parte considerável das organizações ainda não acredita que poderá ser um possível alvo de ataque. Os ciberincidentes poderão atingir custos financeiros de milhões de euros, sendo por isso fundamental analisar e avaliar o potencial impacto que eventuais vulnerabilidades, ameaças ou incidentes poderão ter na reputação, *compliance*, resultados financeiros e serviços da organização (Alahmari e Duncan, 2021).

A Gestão de Riscos de Cibersegurança é um processo que se baseia na identificação e análise dos riscos cibernéticos da organização, providenciando uma avaliação da probabilidade e do impacto dos riscos cibernéticos no negócio, de forma a tomar decisões que permitam mitigar ou eliminar esses riscos (Naseer *et al.*, 2018). "Com base nesta avaliação do risco, os controlos técnicos e processuais são implementados, seguidamente monitorizados, de forma a

medir a eficácia do processo de Gestão de Riscos de Cibersegurança" (Naseer *et al.*, 2018, p.3).

O processo de Gestão de Riscos de Cibersegurança engloba aspetos técnicos, processuais e humanos (Lee, 2021). Sendo o erro humano considerado uma das principais vulnerabilidades de Cibersegurança, é possível perceber a importância que a Gestão de Risco poderá ter na prevenção de diversas vulnerabilidades e ameaças, na medida em que ao identificar e analisar o impacto e a probabilidade da ocorrência dos riscos, poderemos tomar medidas preventivas adequadas de forma a não prejudicar a atividade operacional e os objetivos da organização.

A Gestão de Riscos de Cibersegurança deve permitir às organizações tomar decisões de forma priorizada e informada e estas decisões devem estar orientadas para garantir a Confidencialidade, Disponibilidade e Integridade dos ativos de informação (onde está incluída a informação) e serviços essenciais da organização (Centro Nacional de Cibersegurança de Portugal, 2019). Sendo a TAP um operador de serviços essenciais, o processo de Gestão de Riscos de Cibersegurança deverá estar totalmente integrado e implementado no ambiente da organização, sendo considerado uma parte essencial no sucesso da Cibersegurança deste tipo de organizações (National Institute of *Standards* and Technology, 2018).

Os principais conceitos e respetivas relações de alto nível referentes à Gestão de Riscos de Cibersegurança, estão representados na **Fig.2**, sendo possível sintetizar que a Gestão de Riscos de Cibersegurança pretende garantir a Confidencialidade, Integridade e Disponibilidade dos ativos de Informação, que são cruciais para o desempenho das operações da organização e de extrema importância para os *stakeholders*, através da identificação e análise do impacto e probabilidade de ocorrência de vulnerabilidades que poderão ser exploradas por ameaças, levando a riscos que deverão ser mitigados ou eliminados, através da tomada de decisões de forma priorizada sobre os controlos (técnicos e

processuais) que deverão ser implementados pela organização (Centro Nacional de Cibersegurança de Portugal, 2019).

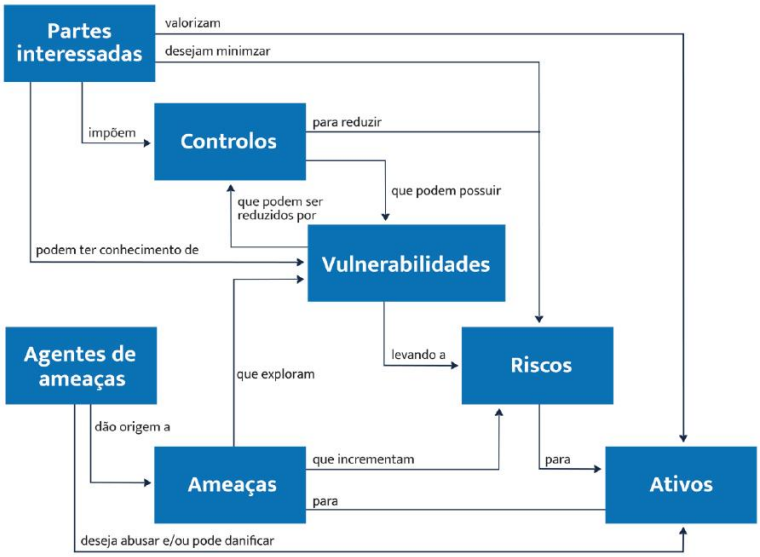


Figura 2 - Conceitos Básicos e Relações de Alto Nível de Gestão de Riscos de Cibersegurança. Fonte: Quadro Nacional de Referência para a Cibersegurança (QNRCS)

As principais atividades realizadas durante o estágio tiveram incidência na TPCRM, nomeadamente, no desenvolvimento de um *Framework* para a Gestão de Riscos de Cibersegurança de Fornecedores, com base na metodologia de gestão de risco que consta na ISO 27005 (International Organization for *Standard*ization, 2018). As fases do processo de Gestão de Riscos de Cibersegurança estão representadas na **Fig. 3**, sendo que o *Framework* incidiu sobre as fases de **Estabelecimento do Contexto**, **Identificação** e **Análise do Risco**.

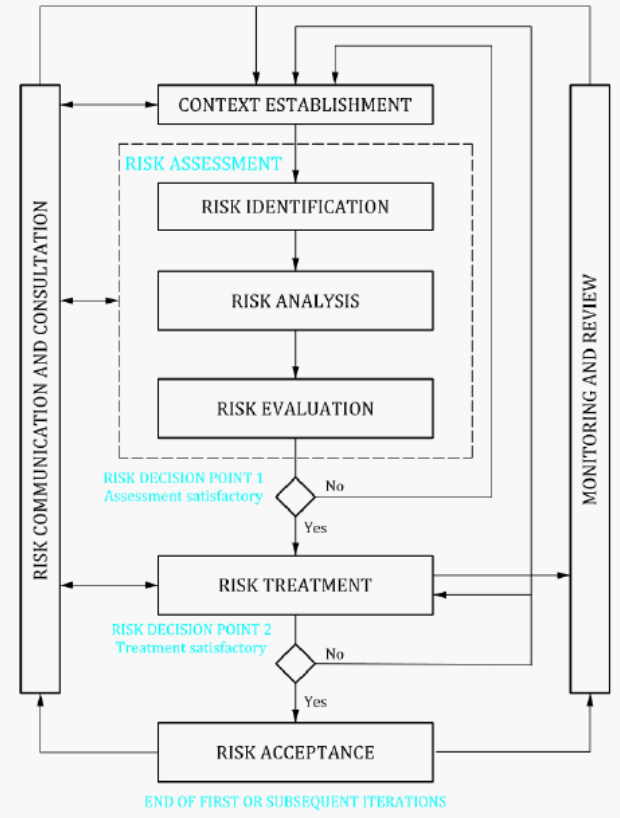


Figura 3 - Processo e Fases da Gestão de Riscos de Cibersegurança. Fonte: ISO 27005

A Gestão de Riscos de Cibersegurança pode ser percecionada como um conjunto coordenado de atividades e processos para gerir e controlar o programa de Cibersegurança de uma organização com base nos riscos cibernéticos identificados, analisados e avaliados (Meszaros e Buchalcevova, 2017). Consequentemente, a utilização de metodologias de identificação, análise e avaliação de risco para avaliar o **programa/plano de Segurança da Informação**[1] (inclui o plano de Cibersegurança) das organizações é uma prática recorrente utilizada para planear, alcançar e manter um nível apropriado de segurança (International Organization for *Standard*ization, 2013). A análise e avaliação do risco é essencial para desenvolver e melhorar as diversas políticas

[1] Denominado na ISO 27001 por ISMS.

de Cibersegurança de uma organização e para uma correta alocação dos recursos limitados com base no investimento planeado em Cibersegurança (Henrie, 2013).

2.4. Gestão de Riscos de Cibersegurança de Fornecedores (TPCRM)

As TIC providenciadas através da cadeia logística oferecem diversos benefícios significativos, tais como, baixo custo, interoperabilidade, rápida inovação e variedade de características dos produtos/serviços. Contudo, os mesmos fatores que criam estes benefícios também aumentam o potencial de riscos de Cibersegurança que surgem direta ou indiretamente da cadeia de fornecimento (Boyens, 2022).

Os ciberincidentes derivados de fornecedores podem provocar graves disrupções na logística, produção e operações, impactando de forma negativa toda a cadeia logística, e consequentemente o nível de serviço providenciado aos clientes (Simon e Omar, 2020). Atualmente, os fornecedores são uma das principais causas que tornam as empresas vulneráveis a um possível ciberincidente (Ex: violação de dados[2]), sendo por isso fundamental implementar e manter processos que garantam a proteção da organização, bem como dos princípios C.I.A potencialmente afetados por riscos de Cibersegurança de fornecedores (Lamba, 2020). Neste sentido, a principal atividade realizada durante o estágio (*Framework* para a Gestão de Riscos de Cibersegurança de Fornecedores) é fundamental para reforçar o nível de segurança e prevenção do atual programa/plano de Segurança da Informação da TAP.

A Gestão de Riscos de Cibersegurança de Fornecedores (TPCRM) é um processo sistemático para gerir a exposição aos riscos de Cibersegurança

[2] Data Breach.

derivados de fornecedores, através do desenvolvimento de estratégias de resposta apropriadas, políticas, processos e procedimentos (Boyens, 2022). Neste sentido, um dos principais objetivos da TPCRM consiste em garantir o controlo de riscos de Cibersegurança de toda a cadeia logística, adotando uma abordagem holística, de forma a contribuir para o aumento da ciber resiliência e capacidade de adaptabilidade contínua da organização (Creazza *et al.*, 2022). A partilha de informações relacionadas com riscos (vulnerabilidades, ameaças, eventos de segurança da informação, incidentes, etc.), entre a empresa e os seus fornecedores, é fundamental para aumentar a eficácia do processo de TPCRM, reduzindo o impacto de possíveis riscos de Segurança de Informação e Cibersegurança de fornecedores (Zeiringer *et al.*, 2022).

TPCRM é um conceito relativamente recente no mundo empresarial. Todos os riscos de Cibersegurança de fornecedores deverão ser geridos corretamente, de forma a prevenir e mitigar potenciais impactos, derivados de ciberincidentes de fornecedores. Com uma TPCRM eficaz, as empresas conseguem mitigar atempadamente e de forma eficaz potenciais vulnerabilidades, ameaças e ciberincidentes derivados de fornecedores (Keskin *et al.*, 2021).

2.5. Estado atual da Cibersegurança no Sector Aeronáutico

A Cibersegurança na aviação é cada vez mais importante, devido ao avanço tecnológico e à inovação que caracterizam este sector, considerando que atualmente todos os sistemas estão interligados devido à facilidade de acesso à Internet, em qualquer tempo e lugar, mesmo em altitudes de cruzeiro de 10668m, podendo este valor variar consoante o modelo da aeronave. “A Cibersegurança na aviação é definida como a forma de proteger os sistemas informáticos contra ciberataques no sector da aviação. Estes sistemas informáticos podem estar em terra, tais como servidores que contenham informações ou sistemas valiosos que coordenam e facilitam as operações de

voo, ou podem estar no ar durante o voo, como por exemplo entretenimento a bordo e *electronic flight bag* (EFB)" (Kagalwalla e Churi, 2019, p.1).

A maior parte dos CEOs das companhias aéreas consideram a Cibersegurança essencial e um dos principais riscos para a organização caso não seja implementada e gerida corretamente, devido à natureza sensível dos sistemas de voo e dos dados dos passageiros (Leo Tong e Ming Kwan, 2022).

O avanço tecnológico e as diversas tecnologias utilizadas (Ex: *Cloud Computing*, *IoT* e *Machine Learning*) permitem às companhias aéreas otimizar os seus processos e compreender melhor os seus clientes, mas também aumentam a superfície de ataque, permitindo que os cibercriminosos tenham mais hipóteses de efetuar ciberataques que possam prejudicar a empresa (Leo Tong e Ming Kwan, 2022).

"Segundo a Avlaw Aviation, um dos ataques mais comuns que ocorrem na indústria da aviação é o ataque distribuído de negação de serviço (DDoS)" (Ishtiaq e Rahman, 2021, p.2). O acesso não autorizado e ataques *man-in-the-middle* (MitM) são exemplos de outros ataques que ocorrem habitualmente no sector da aviação, podendo afetar negativamente a reputação, *compliance*, serviços e resultados financeiros das companhias aéreas (Elmarady e Rahouma, 2021).

A gestão de ameaças e riscos de Cibersegurança é essencial de forma a implementar medidas para reforçar a segurança, garantindo que qualquer ciberataque tenha um efeito mínimo na segurança da aviação civil (Stastny e Stoica, 2022). Consequentemente, é necessário gerir adequadamente todas as ameaças e riscos de Cibersegurança que possam impactar a segurança da aviação civil, considerando os principais sistemas de transporte aéreo que poderão representar graves vulnerabilidades para a segurança dos aviões (Ishtiaq e Rahman, 2021), nomeadamente: *Very High Frequency* (VHF); *Automatic Dependent Surveillance-Broadcast* (ADS-B); Navegação por Satélite (GPS); Sistema de Entretenimento a Bordo. Deverão ainda ser revistos

regularmente os processos de gestão de riscos de Cibersegurança, para monitorizar o estado dos riscos e garantir uma mitigação eficaz dos mesmos.

Os diversos dados dos clientes das companhias aéreas são um ativo crítico de informação e negócio, sobretudo os dados pessoais (PII), devido ao valor que estes representam para as *airlines*, porque contém detalhes que identificam e descrevem os seus passageiros (Matulevičius *et al.*, 2017). De seguida, são apresentados alguns dos dados mais importantes referentes aos passageiros/clientes: Nome; Morada; Número de Telemóvel; Cartões Bancários; Destinos; Reservas; Entre Outros. Uma possível violação destes dados (*Data Breach*) poderá representar graves consequências para a reputação, *compliance* e resultados financeiros das companhias aéreas, pelo que deverá ser assegurada a proteção desta informação, considerando e integrando os riscos associados no processo de Gestão de Riscos de Cibersegurança das *Airlines.*

As vulnerabilidades mais comuns em todos os sectores (indústrias), incluindo o sector aeronáutico, são o erro humano, a *security awareness* dos empregados e os fornecedores das empresas (Ishtiaq e Rahman, 2021). Deverá ser desenvolvida uma cultura de Cibersegurança entre as companhias aéreas e os seus fornecedores, de forma a reduzir a probabilidade de exploração das vulnerabilidades referidas, por exemplo através de programas de sensibilização e formação em Cibersegurança (Kagalwalla e Churi, 2019). As *Airlines* devem assegurar que os seus fornecedores críticos implementam medidas de Cibersegurança adequadas e auditorias de segurança de forma regular, incluindo estes aspetos como requisitos nos contractos com os fornecedores. Para além disso, as práticas de Cibersegurança de todos os fornecedores deverão ser avaliadas regularmente, com o objetivo de detetar potenciais vulnerabilidades, ameaças e riscos. O conhecimento das vulnerabilidades, ameaças e riscos dos respetivos fornecedores, permite que as companhias aéreas possam exigir requisitos de Cibersegurança aos seus fornecedores, com base neste conhecimento e na criticidade do serviço/produto fornecido (Koepsel, 2019). A Gestão de Riscos de Cibersegurança de Fornecedores (TPCRM) é uma

preocupação cada vez maior das companhias aéreas, sendo possível verificar que o sector da aviação está a realizar investimentos significativos e a implementar medidas para gerir os riscos de Cibersegurança derivados de fornecedores (Leo Tong e Ming Kwan, 2022). Uma das principais razões que justificam esta crescente preocupação em gerir os Riscos de Cibersegurança de Fornecedores, está relacionada com o aumento do uso de práticas globais do sector aeronáutico, ou seja, a globalização do sector e utilização das respetivas *Best Practices*, sendo estas geralmente providenciadas/implementadas pelos fornecedores (Koepsel, 2019).

Tendo como base o anterior parágrafo, verifica-se que a implementação de um *Framework* para a Gestão de Riscos de Cibersegurança de Fornecedores é fundamental de modo a reforçar a segurança das companhias aéreas, considerando que os fornecedores representam uma das principais vulnerabilidades em termos de Cibersegurança para as *Airlines*. Neste sentido, a principal atividade realizada durante o estágio (desenvolvimento de um *Framework* para a TPCRM) torna-se essencial para reforçar e aumentar o nível de prevenção, proteção e resiliência do ISMS da TAP Air Portugal.

3. TAP Air Portugal

3.1. Apresentação da Organização

A TAP Air Portugal, sediada em Lisboa, é uma empresa do ramo da aviação comercial, tendo começado recentemente a operar também no ramo da logística de aviação, através da “TAP Air Cargo”. Desde a sua criação, em 1945, que a TAP Air Portugal se rege por altos padrões de profissionalismo, segurança e sustentabilidade, sendo avaliada atualmente como a 5ª companhia aérea mais segura do mundo pela AirlineRatings. A TAP Air Portugal é membro da Star Alliance desde 2005, reforçando assim a sua reputação e estatuto, considerando

que para se tornarem membros desta rede, todas as companhias aéreas devem cumprir com os mais altos padrões da indústria.

A melhoria contínua da sustentabilidade ambiental é uma prioridade, através da redução do consumo de recursos, eficiência no uso de combustível, modernização da frota, gestão de recursos e inovação tecnológica. A TAP Air Portugal pretende reafirmar o seu compromisso com o futuro e o ambiente, ligando pessoas, experiências, comunidades e culturas, afirmando-se cada vez mais como a maior exportadora nacional e um dos símbolos da nossa nação.

3.1.1. Principais Acontecimentos Históricos

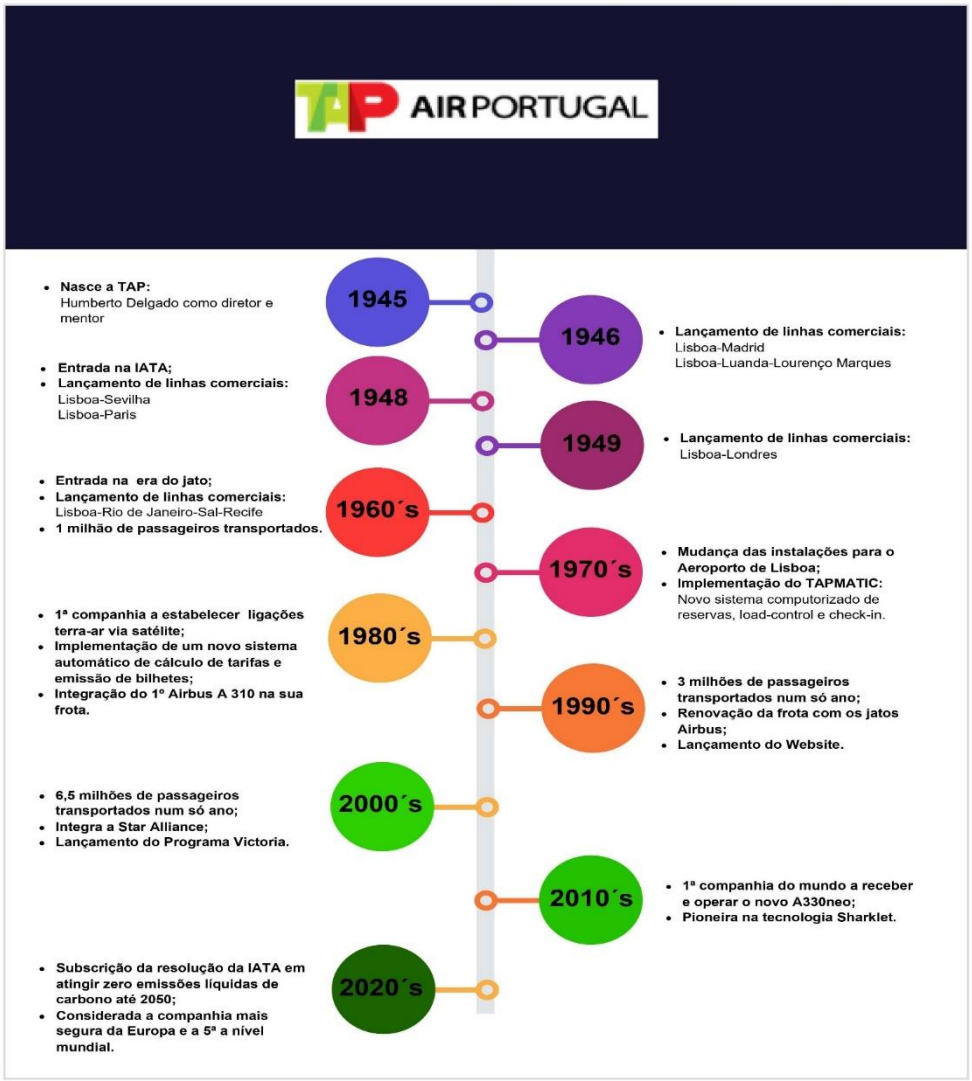


Figura 4 - Cronograma dos Principais Acontecimentos Históricos. Fonte: elaboração própria

3.1.2. Missão, Visão e Valores

A TAP Air Portugal tem como missão garantir a excelência no serviço de transporte aéreo e atividades afins, ligando pessoas, economias e comunidades, afirmando-se cada vez mais como a maior exportadora nacional e promotora de Portugal nos vários continentes do mundo; define como visão "…acredita na interação, no poder de ligar e mover pessoas, trazendo novas possibilidades de um futuro melhor" (TAP Air Portugal, 2023); a companhia baseia toda a sua operação e destaca como valores a **segurança**, **confiança**, **sustentabilidade**, **inovação tecnológica** e **proximidade com o cliente.**

4. Atividades Realizadas no Estágio

No presente capítulo serão descritas todas as atividades realizadas durante o estágio, no departamento de Cibersegurança (*Cybersecurity Services*) da TAP Air Portugal, com destaque para a principal atividade realizada, que consistiu no desenvolvimento de um ***Framework* para a Gestão de Riscos de Cibersegurança de Fornecedores da TAP.**

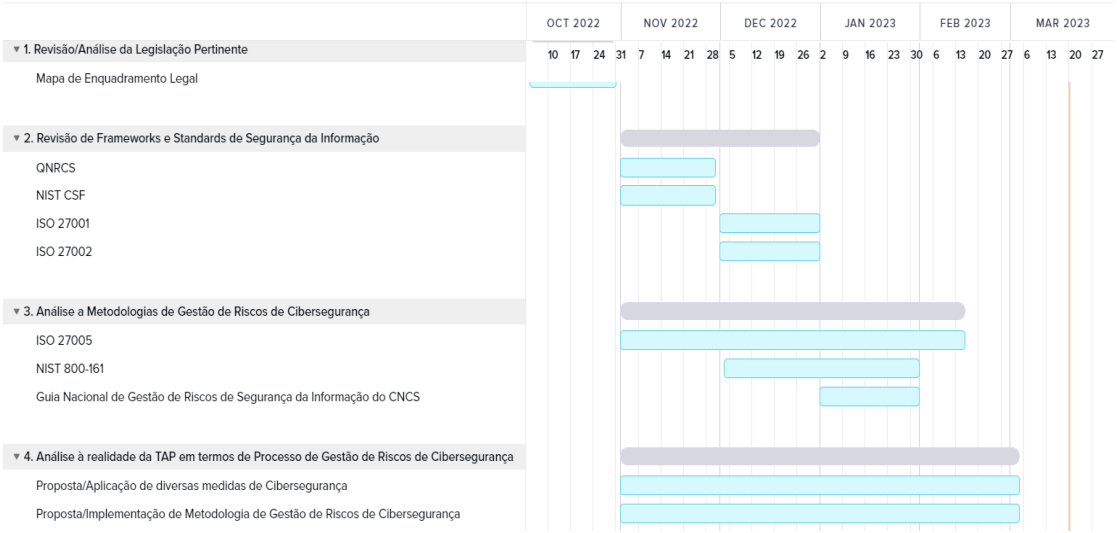


Figura 5 - Atividades Propostas no Plano de Estágio. Fonte: elaboração própria

As atividades descritas no subcapítulo 4.2. “Principais Atividades Desenvolvidas”, estão diretamente relacionadas com as atividades propostas no plano de estágio (**Fig.5**), sendo que, as atividades descritas no subcapítulo 4.3. “Outras Atividades Desenvolvidas”, tiveram como intuito suportar a realização das atividades principais.

4.1. Contextualização do Estágio

O estágio teve a duração de seis meses, iniciando a 3 de outubro de 2022 e com término a 31 de março de 2023, tendo como atividades propostas, as atividades representadas na **Fig. 5**.

As atividades realizadas durante o primeiro mês tiveram como principal objetivo ganhar conhecimento sobre possíveis obrigações legais aplicáveis à TAP Air Portugal, enquanto operador de serviços essenciais. Nos primeiros dias ocorreu também o acolhimento por parte da organização, de forma a conhecer as principais instalações da TAP, entre outros aspetos importantes, sendo ainda entregue um computador portátil e um *Welcome Kit*. Neste mês, realizei ainda todos os cursos (e-learning) de Segurança da Informação oferecidos pela TAP.

Durante o segundo e terceiro meses de estágio, efetuei uma análise crítica a diversos *Frameworks* e *Standards* de Segurança da Informação, com o intuito de perceber os principais domínios (áreas de atuação) de Segurança da Informação, bem como, os controlos técnicos, organizacionais e processuais necessários para implementar e gerir o programa/plano de Segurança da Informação de uma empresa, procurando enquadrar o conhecimento obtido na realização da atividade principal. Nestes dois meses, efetuei também uma análise a metodologias de Gestão de Riscos de Cibersegurança, com base nos principais *Frameworks* e *Standards* de referência, de forma a planear todas as fases, processos e procedimentos necessários para desenvolver e implementar o *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP. É importante referir que neste período, iniciei o desenvolvimento do *Framework*

de TPCRM da TAP, atividade que se estendeu até ao dia 3 de março de 2023, onde realizei uma apresentação presencial para os membros do departamento de Cibersegurança, culminando o trabalho realizado durante o estágio, no sentido de avaliar e discutir a implementação do *Framework* de TPCRM da TAP. Durante o desenvolvimento do *Framework* foram realizadas diversas reuniões pelo Teams com o orientador de estágio na TAP (António Carrilho), sendo o seu *feedback*, sugestões e correções fundamentais, no sentido de me ajudar a desenvolver um *Framework* que permita gerir adequadamente os riscos de Cibersegurança de fornecedores da TAP, garantindo que os riscos mais graves são mitigados atempadamente pelos devidos fornecedores.

Para além das atividades propostas no plano de estágio, também analisei o RGPD, a Diretiva NIS 2 e a Diretriz 2023/1 da CNPD, sendo esta legislação fundamental para garantir a conformidade da Gestão de Riscos de Cibersegurança de Fornecedores com a legislação aplicável, sobretudo quando o fornecedor acede, transmite, gera, mantém ou processa dados pessoais (PII[3]) da responsabilidade da TAP. Adicionalmente, realizei várias tarefas extra que não estavam incluídas nas atividades propostas no plano de estágio, participando ainda de forma ativa em várias tarefas diárias realizadas pelo departamento de Cibersegurança, nomeadamente:

- Correção de conteúdos desatualizados, nas páginas e cursos de Segurança de Informação da Intranet da TAP;
- Utilização do *software* Security Scorecard;
- Outras atividades desenvolvidas, que por motivos de confidencialidade não podem ser relevadas.

[3] Personally identifiable information.

4.2. Principais Atividades Desenvolvidas

4.2.1. Atividade A – Mapa de Enquadramento Legal

A 1ª atividade realizada durante o estágio, teve como principal objetivo realizar um enquadramento legal da principal legislação aplicável à TAP, enquanto operador de serviços essenciais, sendo essencial no sentido de me facultar uma visão geral dos principais aspetos legais referentes a Segurança da Informação e Cibersegurança em Portugal e na União Europeia.

De seguida, foram desenvolvidos 3 quadros (Anexo I e II), com o intuito de realizar um resumo das principais obrigações identificadas no DL nº65/2021[4] e na Diretiva NIS[5]. Todas as obrigações apresentadas nestes 3 quadros são cumpridas rigorosamente pela TAP, sendo importante destacar as obrigações relacionadas com Gestão de Riscos, porque são fundamentais de forma a garantir que o processo de Gestão de Riscos de Cibersegurança é realizado garantindo *compliance* com a legislação aplicável.

A realização desta atividade foi fundamental para obter uma visão geral das principais obrigações legais da TAP, enquanto operador de serviços essenciais, e para compreender em que se baseia o panorama legal de Segurança da Informação e Cibersegurança, sendo este aspeto crucial na definição e desenvolvimento da estratégia de Segurança da Informação da empresa.

[4] Regime Jurídico da Segurança do Ciberespaço.

[5] Medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia

4.2.2. Atividade B - Análise crítica de *Frameworks* e *Standards* relacionados com Segurança da Informação e Cibersegurança

Um dos aspetos fundamentais da Segurança da Informação e Cibersegurança é perceber que *Frameworks* e *Standards* deverão ser usados para implementar de forma apropriada a estratégia e plano/programa de Segurança da Informação das empresas. Neste sentido, com base no seu perfil de risco, legislação aplicável e obrigações contratuais, cada organização deverá decidir que *Frameworks* e *Standards* se adequam melhor ao seu modelo e objetivos de negócio, de forma a garantir a resiliência das suas operações e a proteção dos ativos de informação.

Foram analisados detalhadamente os seguintes *Frameworks* e *Standards*:

- NIST CSF;
- QNRCS;
- ISO 27001;
- ISO 27002.

Relativamente aos ***Frameworks* NIST CSF e QNRCS**, é possível constatar que são bastante semelhantes, tendo como principal foco a implementação de diversos controlos (técnicos, organizacionais e processuais) de segurança em operadores de infraestruturas críticas e serviços essenciais, considerando a Gestão de Riscos de Cibersegurança como uma das bases do programa de Segurança da Informação da empresa. O Core destes dois *Frameworks*, é baseado nos 5 objetivos de Cibersegurança (Identificar, Proteger, Detetar, Responder e Recuperar), em que para cada um são apresentados diversos controlos de segurança de forma a garantir que estes objetivos são devidamente cumpridos. Através da análise crítica realizada a estes *Frameworks*, consegui obter uma perceção geral das principais áreas de atuação da Cibersegurança e dos controlos de segurança que deverão ser implementados para proteger, redes, computadores/sistemas,

programas/aplicações e informação, de ataques e danos ou de acesso não autorizado, garantindo a preservação da Confidencialidade, Integridade e Disponibilidade da informação da organização.

Quanto aos ***Standards* ISO 27001 e 27002**, são provavelmente os mais utilizados na indústria para desenvolver, implementar e manter o programa de Segurança da Informação das empresas (ISMS), devendo ser utilizados em conjunto, i.e., deverão utilizar-se os controlos específicos de segurança da ISO 27002 para implementar os requisitos e controlos de referência de Segurança da Informação da ISO 27001. No entanto, importa enfatizar que as organizações podem combinar estas ISOs com outros *Frameworks* para implementar o seu ISMS, garantindo uma maior cobertura e eficácia do seu programa de *InfoSec*. A análise crítica realizada às ISO 27001 e 27002, foi fulcral no desenvolvimento do *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP, especificamente, na definição dos requisitos de Cibersegurança e na criação de um questionário para avaliar as práticas de Cibersegurança dos fornecedores, de modo a identificar potenciais vulnerabilidades, ameaças ou cenários de incidente de fornecedores que possam impactar a TAP.

4.2.3. Atividade C – Análise a Metodologias de Gestão de Riscos de Cibersegurança

A análise a metodologias de Gestão de Riscos de Cibersegurança foi fundamental, de modo a planear/estruturar o *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP. Neste sentido, foram analisados 3 *Frameworks*/*Standards*: **ISO 27005**; **NIST 800-161**; **Guia Nacional de Gestão de Riscos de Segurança da Informação do CNCS**.

De seguida, na Atividade D, será identificado e descrito o principal propósito da utilização e análise dos *Frameworks*/*Standards* referidos no parágrafo anterior.

4.2.4. Atividade D – Desenvolvimento e Implementação do *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP

4.2.4.1. Etapa 0 – Síntese dos conceitos fundamentais e definição das etapas

De forma a iniciar o desenvolvimento do *Framework* para a Gestão de Riscos de Cibersegurança de Fornecedores de TIC da TAP, realizei uma síntese dos conceitos fundamentais e uma atualização legal da nova Diretiva NIS 2 no contexto da Gestão de Riscos de Cibersegurança de Fornecedores. Foram também definidas as principais etapas/passos para desenvolver e implementar o *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP.

Um fornecedor, é definido neste contexto, como uma organização que fornece um produto/serviço de TIC ou que usa recursos eletrónicos da TAP para este propósito, por exemplo a utilização de dados pessoais da responsabilidade da TAP.

A recém-publicada diretiva NIS 2, no artigo 21º, indica que a TAP deverá implementar medidas técnicas, operacionais e organizacionais que permitam gerir os riscos de Segurança da Informação, devendo estas incluir a segurança da cadeia logística. A TAP deve considerar as vulnerabilidades e ameaças especificas de cada fornecedor, sendo por isso fundamental desenvolver um *Framework* para a Gestão de Riscos de Cibersegurança de Fornecedores.

O *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP é baseado na metodologia de Gestão de Riscos presente na ISO 27005, representada na **Fig.3**. É importante referir que o *Framework* desenvolvido incide sobretudo nas fases de **Estabelecimento do Contexto**, **Identificação do Risco** e **Análise do Risco**, sendo que o Tratamento do risco é da responsabilidade dos fornecedores e as restantes fases apenas deverão ser consideradas aquando da implementação do *Framework*.

O principal objetivo deste *Framework* é determinar o nível de risco de possíveis riscos de fornecedores, ou seja, determinar a probabilidade de ocorrência e o impacto dos mesmos, de forma a definir a priorização do tratamento de risco. Apesar do tratamento do risco ser da responsabilidade dos fornecedores, a TAP deverá estabelecer a priorização para tratamento do risco consoante o nível de risco para a organização e possíveis impactos, certificando-se que riscos mais graves são mitigados pelos devidos fornecedores. O objetivo final do *Framework* é integrar este processo na Gestão de Riscos de Cibersegurança da TAP.

Por último, foram definidos os principais passos/etapas para desenvolver e implementar o *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP (Anexo III). A **1ª etapa** traduz-se no estabelecimento de 2 *TIERS* de Classificação de Risco para enquadrar fornecedores segundo o impacto que poderão provocar na TAP. **De seguida**, foram definidos requisitos de Cibersegurança e um questionário para avaliar as práticas de Cibersegurança dos fornecedores, de modo a identificar possíveis riscos. A **3ª etapa** consiste em implementar o processo interno para avaliar e analisar os riscos. Quanto aos próximos passos, representam os aspetos a considerar após implementar o *Framework*.

4.2.4.2. Etapa 1 – Definição de *TIERS* de Classificação de Risco e respetivo processo de classificação de fornecedores.

A **1ª etapa** para desenvolver e implementar o *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP, consiste na definição de ***TIERS* de Classificação de Risco e o respetivo processo de classificação de fornecedores.** Os *TIERS* de Classificação de Risco enquadram-se na fase de Estabelecimento do Contexto, sendo que o principal objetivo da sua criação é simplificar o processo geral de gestão de riscos, tornando mais fácil a identificação, análise e avaliação dos riscos dos fornecedores conforme o *TIER* em que estão classificados.

Foram definidos **2 *TIERS* de Classificação de Riscos** (Anexo IV). O ***TIER* 1** refere-se a fornecedores críticos, ou seja, que fornecem um produto/serviço crítico para a TAP ou que têm acesso, transmitem, gerem, mantêm ou processam dados pessoais da responsabilidade da TAP, podendo representar riscos médios ou elevados e ter impacto médio/elevado na reputação, *compliance*, resultados financeiros ou serviços da TAP. Por outro lado, o ***TIER* 2** refere-se aos restantes fornecedores que podem representar riscos médios ou baixos e causar impacto médio/baixo na TAP. Para fornecedores do TIER 1 deverão ser definidos requisitos de Cibersegurança mais exigentes que deverão ser auditados regularmente. O departamento de Cibersegurança da TAP deverá assegurar que os fornecedores do *TIER* 1 mitigam os seus riscos atempadamente. Após definir os *TIERS* de classificação de risco, é necessário desenvolver um processo que permita classificar os fornecedores nos *TIERS* definidos.

A classificação dos fornecedores começa pelo preenchimento de um quadro referente a aspetos gerais do fornecedor (Anexo V). De seguida, o assessor da TAP deve responder a duas questões críticas para classificar o fornecedor (Anexo VI). Se a resposta for negativa em ambas as questões o fornecedor é classificado no *TIER* 2. Se pelo menos uma das respostas for positiva, o fornecedor é classificado no *TIER* 1 (crítico). Para os fornecedores do *TIER* 1, deverá ser feita uma análise detalhada sobre os possíveis impactos e os princípios C.I.A potencialmente afetados por cenários de ciberincidentes de fornecedores. A análise detalhada dos fornecedores do *TIER* 1 (Anexo VII), envolve identificar e analisar o potencial impacto de cenários de incidente de fornecedores nos serviços, resultados financeiros e reputação da TAP. O impacto em termos de *compliance* deverá ser analisado separadamente, sobretudo quando o fornecedor acede, transmite, gera, mantem ou processa dados pessoais, devido às graves consequências que uma possível violação deste tipo de dados poderá ter. Deverão ainda ser considerados os princípios C.I.A potencialmente afetados por estes incidentes, de modo a propor medidas

que possam reforçar a proteção destes princípios e a resiliência da Cibersegurança da TAP.

Por último o fornecedor deverá ser registado num dos *templates* criados para o efeito, sendo que neste relatório apenas considero necessário apresentar o *template* para classificação de fornecedores do *TIER* 1 (Anexo VIII).

Com o intuito de exemplificar o processo de classificação de fornecedores, de seguida é apresentado um resumo deste processo para 2 fornecedores, um do *TIER* 1 e outro do *TIER* 2. A Amadeus que suporta e providencia o sistema de reservas para a TAP, é considerado um fornecedor crítico (*TIER* 1). Seguindo a metodologia referida anteriormente, os serviços/produtos providenciados pela Amadeus têm acesso a sistemas críticos da TAP que transmitem, gerem ou processam dados pessoais, para além de também suportarem processos de negócio críticos, sendo assim classificado como um fornecedor do *TIER* 1. A SonarSource que providencia a aplicação SonarQube, utilizada para inspeção contínua da qualidade de linguagem de programação, é considerado um fornecedor não crítico (*TIER* 2). Considerando que não tem acesso a sistemas da TAP que transmitem, gerem ou processam dados pessoais, nem suporta ou executa um processo de negócio crítico, é classificado como um fornecedor do *TIER 2.*

4.2.4.3. Etapa 2 – Identificação do Risco

A **2ª etapa** para desenvolver e implementar o *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP, consiste na **identificação do risco**, que será realizada através da **avaliação de requisitos de Cibersegurança** e de um **questionário** a realizar aos fornecedores.

Foram definidos **requisitos de Cibersegurança**, com base na ISO 27001 (não serão apresentados neste relatório por ser uma lista demasiado extensa), de modo a identificar potenciais vulnerabilidades, ameaças ou cenários de incidente que possam impactar a TAP. Todos os Requisitos de Cibersegurança do *TIER* 2 sendo mais básicos aplicam-se também ao *TIER* 1, porque foi definido

anteriormente que os requisitos teriam de ser mais exigentes para fornecedores do *TIER*. 1, logo os requisitos mais básicos devem ser cumpridos por todos os fornecedores. Os requisitos de Cibersegurança estão segregados em requisitos de Cibersegurança gerais, requisitos de controlos de Cibersegurança (retirados dos controlos do anexo A da ISO 27001) e requisitos de controlos de Cibersegurança por domínio de Segurança da Informação.

De seguida, foi desenvolvido um **questionário** com o intuito de suportar a avaliação dos requisitos de Cibersegurança previamente definidos, de forma que com ambos seja possível identificar potenciais vulnerabilidades, ameaças e cenários de incidente que possam impactar a TAP. As principais fontes utilizadas para realizar este questionário foram o *Framework* NIST 800-161, o RGPD e a nova Diretriz 2023/1 (relativa a medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais). Importa referir que existem 2 tipos possíveis de questionários, um para fornecedores do *TIER* 1 e outro para fornecedores do *TIER* 2. No caso de o fornecedor ser crítico (*TIER* 1) e aceder, transmitir, gerar, manter ou processar dados pessoais, deverão ser incluídas as questões do anexo A ao questionário de fornecedores do *TIER* 1. O questionário está dividido em domínios de Segurança da Informação relacionados com os domínios em que também estavam divididos os requisitos de Cibersegurança. É essencial que a TAP assegure que todos os fornecedores do *TIER* 1 preenchem o questionário, através da inclusão desta obrigação nos acordos contratuais com os fornecedores.

Os questionários por motivos de confidencialidade não serão apresentados neste relatório, porque estão associados a um dos atuais processos de TPCRM da TAP.

4.2.4.4. Etapa 3 – Análise do Risco

A **3ª etapa**, ou seja, a **análise do risco** é considerada a fase mais importante do *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP.

O **processo de análise de risco** (Anexo IX) começa com a **identificação dos ativos de informação** que poderão ser afetados por potenciais cenários de incidentes de fornecedores. Seguidamente, é necessário **definir um cenário de incidente**, usando um dos seguintes métodos. O **método A**, consiste em identificar uma vulnerabilidade e uma ameaça que a possa explorar, por exemplo através da utilização das fontes apresentadas, sendo que a 1ª fonte corresponde a uma lista de todas as vulnerabilidades conhecidas até à data com o respetivo score cvss e a 2ª fonte corresponde a uma lista de vulnerabilidades e ameaças que desenvolvi com base na ISO 27005 e outros *Frameworks* de referência. O **método B**, consiste em definir diretamente um cenário de incidente através da taxonomia de referência de incidentes do CNCS. Após definir o cenário de incidente, **é necessário atribuir um valor de cálculo ao impacto da concretização deste cenário de incidente e á sua probabilidade de ocorrência**. A multiplicação do valor de cálculo do impacto pelo valor de cálculo da probabilidade de ocorrência traduz-se no **nível de risco**. Por último, o risco deverá ser registado na tabela de registo de riscos, que será explicada com maior detalhe através de exemplos práticos.

Os critérios de impacto já tinham sido definidos anteriormente pela TAP, e também se considerou que fornecedores do *TIER* 1 poderiam provocar um impacto médio/elevado, enquanto fornecedores do *TIER* 2 poderiam provocar um impacto médio/baixo. Os critérios de probabilidade de ocorrência (Anexo X) foram definidos com base no guia nacional de gestão de riscos de segurança da informação do CNCS e no *Framework* NIST 800-30 (NIST *Risk Assessment*). Para cada nível de impacto e classificação de probabilidade de ocorrência existe um valor de cálculo correspondente que deverá ser utilizado para calcular o nível de risco. É importante referir que se o cenário de incidente afetar mais do que uma categoria de impacto ou tiver mais do que uma classificação de probabilidade de ocorrência, ou seja, mais do que 1 valor possível de cálculo, considera-se sempre o maior valor de cálculo para registar o risco. Por exemplo, se um cenário de incidente tiver um impacto moderado com um valor de cálculo

5 em termos de serviço, mas um impacto catastrófico em termos de *compliance* com um valor de cálculo 9, considera-se sempre o maior valor de cálculo, neste exemplo o valor 9.

A 1ª tabela apresentada no Anexo XI explica os critérios utilizados para obter os valores de cálculo. Foram atribuídos intervalos de valores a cada nível de impacto e classificação de probabilidade de ocorrência, de forma a utilizar a mediana desses intervalos como o valor de cálculo para calcular o nível de risco. O nível de risco é obtido através da multiplicação do valor de cálculo do impacto pelo valor de cálculo da probabilidade de ocorrência. **O nível de risco varia entre 1 e 81**, sendo que fornecedores do *TIER* 2 enquadram-se nos níveis 5,3,4, enquanto fornecedores do *TIER* 1 enquadram-se em todos os níveis dependendo do incidente em questão. Isto significa, tal como referi anteriormente, que os fornecedores do *TIER* 1 podem provocar impactos médios ou elevados, sendo possível obter qualquer nível de risco consoante o valor de cálculo da probabilidade de ocorrência. Por outro lado, os fornecedores do *TIER* 2 podem provocar impactos baixos ou médios, sendo possível obter apenas os níveis de risco insignificante, baixo ou moderado.

Para facilitar a compreensão do processo de análise de riscos, desenvolvi 2 exemplos práticos (Anexo XII), para explicar os 2 métodos de definição de cenários de incidente referidos anteriormente. No **exemplo A**, para um fornecedor do *TIER* 1, o cenário de incidente é definido através da identificação de uma vulnerabilidade e da respetiva ameaça que a pode explorar, traduzindo-se num cenário de incidente. Hipoteticamente, considerou-se que o ativo de informação, neste caso, a plataforma de gestão de projetos partilhada entre a TAP e um fornecedor, poderia ser afetada devido a uma vulnerabilidade existente de uma política de palavras-passes insegura, que pode ser explorada por um ataque de força bruta às palavras-passes, resultando assim no comprometimento de uma conta privilegiada. Este cenário de incidente afetaria certamente a confidencialidade e a integridade, e por ser uma conta com direitos privilegiados o valor de cálculo do impacto seria 7 e a probabilidade de

ocorrência seria muito alta, ou seja, um valor de cálculo 9. O valor de risco é igual a 63, sendo assim considerado um risco de nível elevado, ou seja, de nível 2. No **exemplo B**, para um fornecedor do *TIER* 2, o cenário de incidente é definido através da identificação direta de um cenário de incidente, semelhante ao anterior, mas neste caso o comprometimento de uma conta não privilegiada. Hipoteticamente, considerou-se que o ativo de informação, a plataforma de gestão de projetos partilhada entre a TAP e um fornecedor, poderia ser afetada através do comprometimento de uma conta não privilegiada. Este cenário de incidente afetaria a confidencialidade e a integridade, e por ser uma conta com direitos não privilegiados o valor de cálculo do impacto seria 3 e a probabilidade de ocorrência seria alta, ou seja, com um valor de cálculo 7. O valor de risco é igual a 21, sendo assim considerado um risco de nível menor, ou seja, de nível 4.

4.3. Outras Atividades Desenvolvidas

4.3.1. Atividade E - Formação em Segurança da Informação (e-learning – Universidade TAP)

Uma das primeiras atividades efetuadas consistiu em realizar todos os cursos (e-learning) de Segurança da Informação oferecidos pela TAP, de modo a ganhar uma noção ampla das suas principais políticas, normas e procedimentos de Segurança da Informação que suportam o ISMS da organização. Os cursos de e-learning facultados pela TAP, referentes a *InfoSec* são os seguintes:

- Sistema de Gestão da Segurança da Informação (ISMS);
- Classificação da Informação;
- Utilização de Recursos Eletrónicos (Computadores; Correio eletrónico, internet e plataformas; Secretária limpa e Ecrã limpo; Teletrabalho e Equipamentos pessoais);

- Segurança das Passwords e Log-on;
- Phishing.

4.3.2. Atividade F - Security Scorecard

O Security Scorecard é uma ferramenta utilizada para avaliar e melhorar o estado e as práticas de Cibersegurança das organizações, garantir *compliance* com as leis e regulamentos aplicáveis, monitorizar o estado de cibersegurança dos fornecedores, entre outros, permitindo que a TAP controle e reduza o seu nível de risco geral. Esta ferramenta permite que cada organização obtenha o seu *Scorecard* e crie portfolios englobando os seus fornecedores, de forma a monitorizar a evolução do estado de Cibersegurança da empresa e de toda a sua cadeia logística.

Adicionalmente, a TAP utiliza o Security Scorecard para realizar um *benchmark* com o Scorecard de outras Airlines, no sentido de comparar o seu atual nível de risco geral com as outras companhias áreas e também para monitorizar continuamente o nível de risco das empresas subsidiárias do grupo TAP (PGA e UCS).

Durante o estágio, utilizei esta ferramenta como complemento ao *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP, permitindo automatizar parcialmente o processo de TPCRM (nomeadamente, através do envio dos questionários para os fornecedores), explorar a superfície de ataque da TAP e verificar os principais grupos de fatores de risco que afetam negativamente ou positivamente o score atribuído à TAP e aos seus fornecedores, nomeadamente: *DNS health*; IP *reputation*; *Web application security*; *Network security*; *Leaked information*; *Hacker chatter*; *Endpoint security*; *Patching cadence*; *Cubit score*; *Social engineering*.

5. Reflexão Crítica

5.1. Confronto do Enquadramento Teórico com as Atividades Realizadas no Estágio

O estágio na TAP Air Portugal permitiu-me colocar em prática num contexto laboral, o conhecimento teórico adquirido através dos conceitos definidos no enquadramento teórico, incluindo a aprendizagem obtida na unidade curricular de Redes e Segurança de Sistemas de Informação do mestrado.

Quanto à Segurança da Informação, com base na revisão e análise de diversos artigos científicos, conclui-se que o seu principal objetivo passa por garantir a preservação da Confidencialidade, Integridade e Disponibilidade (Tríade C.I.A) da informação. A Tríade C.I.A é uma constante inerente à *InfoSec* e Cibersegurança, tendo diversas aplicações possíveis, como por exemplo, na análise detalhada aos fornecedores do *TIER* 1, onde se considerou os princípios C.I.A potencialmente afetados por cenários de ciberincidentes de fornecedores, de modo a propor medidas que possam reforçar a proteção destes princípios e a resiliência da Cibersegurança da TAP.

A Cibersegurança é um subconjunto da *InfoSec*, podendo ser definida de forma semelhante à Segurança da Informação, mas com âmbito apenas no ciberespaço. Tal como referido no Capítulo I, a definição de Cibersegurança tem sofrido algumas adaptações, sendo considerada por alguns especialistas como a abordagem e as ações associadas com os processos de Gestão de Riscos de Cibersegurança seguidas pelas organizações, tendo como principal objetivo a proteção da Confidencialidade, Integridade e Disponibilidade dos dados e dos ativos no ciberespaço (Kianpour et al., 2022). Consequentemente, o desenvolvimento e implementação do *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores, permitirá elevar o nível de prevenção de Cibersegurança, através da implementação deste processo na Gestão de Riscos

de Cibersegurança da TAP, tornando possível gerir um maior número de riscos cibernéticos.

A Gestão de Riscos de Cibersegurança é um processo que engloba aspetos técnicos, processuais e humanos (Lee, 2021), que consiste em identificar e analisar os riscos de Cibersegurança da organização, permitindo a tomada de decisões de forma priorizada e informada, devendo estas decisões estar orientadas para garantir a proteção dos princípios C.I.A. A metodologia utilizada para o *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP é baseada essencialmente na identificação e análise dos riscos cibernéticos, enquadrando-se desta forma no que é referido no Capítulo I.

Relativamente à TPCRM, em consonância com o que é referido no enquadramento teórico, permite que os riscos de Cibersegurança derivados de fornecedores sejam devidamente geridos, contribuindo para a resiliência e capacidade de adaptabilidade contínua da organização, visto que o *Framework* desenvolvido consiste num processo iterativo e contínuo, tendo como objetivo final integrar o mesmo na Gestão de Riscos de Cibersegurança da TAP, reduzindo desta forma o nível geral de risco da organização. Apesar da TPCRM ser um conceito relativamente recente no mundo empresarial, existe uma certa urgência em implementar um processo que permita gerir os riscos de Cibersegurança de fornecedores, devido ao crescente nº de ciberincidentes que ocorreram ultimamente, sendo por isso fundamental a implementação do *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP.

Os conteúdos do mestrado aplicáveis ao estágio, foram essenciais para desenvolver o *Framework*, nomeadamente, na criação das perguntas para o questionário a realizar aos fornecedores. Neste sentido, de forma a endereçar diversos controlos de cibersegurança, é necessário compreender o funcionamento do modelo OSI e os principais protocolos de segurança, destacando: SSL; TLS; IPsec. Para além disso, algumas das perguntas realizadas no questionário, implicam a compreensão de algoritmos e técnicas de encriptação, tipos de *firewall*, entre outros, sendo por isso o conhecimento obtido

na unidade curricular de Redes e Segurança de Sistemas de Informação fundamental para o desenvolvimento do *Framework* de Gestão de Riscos de Cibersegurança de Fornecedores da TAP.

Relacionando o estado atual ("*As-Is*") da Cibersegurança no sector aeronáutico com a principal atividade desenvolvida durante o estágio (*Framework* para a TPCRM), verifica-se que o departamento de Cibersegurança da TAP acompanha a tendência atual do crescente investimento por parte das *Airlines* em Cibersegurança, nomeadamente em matérias de Gestão de Riscos de Cibersegurança, incluindo os riscos de Cibersegurança de fornecedores. Neste sentido, o desenvolvimento do *Framework* de TPCRM da TAP foi de extrema importância para a organização, considerando que os seus fornecedores, sobretudo os críticos (*TIER* 1), são umas das principais vulnerabilidades em termos de Cibersegurança, e por esse motivo tornou-se necessário implementar um novo processo que permitisse gerir de forma adequada as principais vulnerabilidades, ameaças e riscos provenientes de fornecedores. Tal como referido no subcapítulo 2.2, as práticas de Cibersegurança de todos os fornecedores deverão ser avaliadas e auditadas regularmente, sendo que para este efeito foram desenvolvidos requisitos de Cibersegurança e um questionário, permitindo assim identificar potenciais riscos cibernéticos. Para além disso, também se considerou no *Framework* de TPCRM, que para fornecedores críticos deveriam ser definidos requisitos de Cibersegurança mais exigentes que devem ser auditados regularmente. Em síntese, conclui-se que o ISMS da TAP Air Portugal está em consonância com o estado atual da Gestão de Riscos de Cibersegurança de Fornecedores no sector aeronáutico.

6. Considerações Finais

6.1. Apreciação Pessoal da Experiência de Estágio

O estágio realizado na TAP Air Portugal foi uma experiência extremamente enriquecedora, quer a nível pessoal, quer a nível profissional, permitindo adquirir novas aptidões em *InfoSec* e Cibersegurança, sendo que antes do estágio não tinha qualquer experiência e apenas possuía conhecimentos básicos referentes a estes domínios. O acompanhamento por parte da equipa de Cibersegurança da TAP foi essencial, no sentido de esclarecer dúvidas que foram surgindo e na integração das suas atividades diárias. Destaco a mentoria por parte do meu orientador de estágio na TAP (António Carrilho), que esteve sempre disponível para dar o seu *feedback* e acompanhar o trabalho que fui realizando, sendo este aspeto crucial para obter as bases e competências necessárias de forma a realizar um trabalho congruente e ganhar uma visão geral das principais "*Best-Practices*" que deverão ser utilizadas para garantir a Segurança da Informação.

O ambiente de trabalho na TAP Air Portugal e a flexibilidade em termos de horário, foram imprescindíveis para facilitar a minha integração na organização e conciliar a componente curricular com a realização do estágio, sobretudo durante a época de exames.

Esta experiência na TAP foi fundamental de forma a decidir o rumo profissional que pretendo seguir, ou seja, iniciar uma carreira em Segurança da Informação e Cibersegurança.

6.2. Limitações

Dado que o plano de estágio foi cumprido rigorosamente, apenas identifiquei como limitação no período de estágio o facto de não ter acesso a certo tipo de informações devido a restrições de cariz confidencial (Ex: inventário

de ativos de informação, relatório anual de Cibersegurança da TAP). Também por motivos de confidencialidade, algumas das atividades realizadas durante o estágio não puderam ser descritas neste relatório, por se tratar de operações diárias realizadas pelo departamento de Cibersegurança.

6.3. Sugestões de Melhoria

Tendo como base o âmbito (TPCRM) das principais atividades realizadas no estágio, considero existirem duas melhorias que poderão ser aplicadas para reforçar a importância e melhorar a Gestão de Riscos de Cibersegurança de Fornecedores da TAP:

1. Melhorar a utilização da ferramenta Security Scorecard, incorporando no portfolio atual da TAP todos os fornecedores críticos (*TIER* 1), sendo que atualmente apenas se encontram inseridos um nº limitado de fornecedores;
2. Criação de curso de e-learning sobre TPCRM específico para colaboradores que trabalham na área de (e)*procurement* da TAP, para que tenham noção dos principais riscos cibernéticos e cuidados que deverão ter ao adquirir novos produtos/serviços (TIC) de fornecedores.

Referências Bibliográficas

Alahmari, A. A., and Duncan, R. A. (2021) Towards Cybersecurity Risk Management Investment: A Proposed Encouragement Factors *Framework* for SMEs. In: *2021 IEEE International Conference on Computing (ICOCO)*. IEEE https://doi.org/10.1109/ICOCO53166.2021.9673554.

AlGhamdi, S., Win, K. T., and Vlahu-Gjorgievska, E. (2020) Information security governance challenges and critical success factors: Systematic review. *Computers & Security* 99 102030. https://doi.org/10.1016/j.cose.2020.102030.

Antunes, M., Maximiano, M., Gomes, R., and Pinto, D. (2021) Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy* 1, (2) 219–238. https://doi.org/10.3390/jcp1020012.

Boyens, J. M. (2022) *Cybersecurity Supply Chain Risk Management for Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-161r1.

Centro Nacional de Cibersegurança de Portugal (2019) Quadro Nacional de Referência para a Cibersegurança (QNRCS).

Craigen, D., Diakun-Thibault, N., and Purse, R. (2014) Defining Cybersecurity. *Technology Innovation Management Review* 4, (10) 13–21. https://doi.org/10.22215/timreview/835.

Creazza, A., Colicchia, C., Spiezia, S., and Dallari, F. (2022) Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal* 27, (1) 30–53. https://doi.org/10.1108/SCM-02-2020-0073.

Elmarady, A. A., and Rahouma, K. (2021) Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment. *IEEE Access* 9. https://doi.org/10.1109/ACCESS.2021.3121230.

Guo, M. (2018) China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces. *International Journal of Critical Infrastructure Protection* 22 139–149. https://doi.org/10.1016/j.ijcip.2018.06.006.

Henrie, M. (2013) Cyber Security Risk Management in the SCADA Critical Infrastructure Environment. *Engineering Management Journal* 25, (2) 38–45. https://doi.org/10.1080/10429247.2013.11431973.

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements.*

ISO/IEC 27005:2018, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks.*

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls.*

Ishtiaq, S., and Rahman, N. A. A. (2021) Cybersecurity Vulnerabilities and Defence Techniques in Aviation Industry. https://doi.org/10.2991/ahis.k.210913.071.

Kagalwalla, N., and Churi, P. P. (2019) Cybersecurity in Aviation : An Intrinsic Review. In: *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*. IEEE https://doi.org/10.1109/ICCUBEA47591.2019.9128483.

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., and Tatar, U. (2021) Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. *Electronics* 10, (10) 1168. https://doi.org/10.3390/electronics10101168.

Kianpour, M., Kowalski, S. J., and Øverby, H. (2022) Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory* 116 102493. https://doi.org/10.1016/j.simpat.2022.102493.

Koepsel, K. (2019) *Supply Chain Vulnerabilities Impacting Commercial Aviation*. SAE International https://doi.org/10.4271/9780768093988.

Lamba, A. (2020) 8 Steps to Protect Against Rising Third Party Cyber Risks. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3514893.

Lee, I. (2021) Cybersecurity: Risk management *Framework* and investment cost analysis. *Business Horizons* 64, (5) 659–671. https://doi.org/10.1016/j.bushor.2021.02.022.

Leo Tong, and Ming Kwan (2022) ENSURING CYBER SECURITY IN AIRLINES TO PREVENT DATA BREACH. *Computer Science & IT Research Journal* 3, (3). https://doi.org/10.51594/csitrj.v3i3.426.

Matulevičius, R., Norta, A., Udokwu, C., and Nõukas, R. (2017) Assessment of Aviation Security Risk Management for Airline Turnaround Processes. https://doi.org/10.1007/978-3-662-56266-6_6.

Meszaros, J., and Buchalcevova, A. (2017) Introducing OSSF: A *Framework* for online service cybersecurity risk management. *Computers & Security* 65 300–313. https://doi.org/10.1016/j.cose.2016.12.008.

Naseer, H., Ahmad, A., Maynard, S., and Shanks, G. (2018) Cybersecurity Risk Management Using Analytics: A Dynamic Capabilities Approach. In: *ICIS Proceedings 4*.

National Institute of *Standards* and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Gaithersburg, MD https://doi.org/10.6028/NIST.CSWP.04162018.

Paté-Cornell, M. -Elisabeth, Kuypers, M., Smith, M., and Keller, P. (2018) Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis* 38, (2) 226–241. https://doi.org/10.1111/risa.12844.

Simon, J., and Omar, A. (2020) Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research* 282, (1) 161–171. https://doi.org/10.1016/j.ejor.2019.09.017.

Stastny, P., and Stoica, A.-M. (2022) Protecting aviation safety against cybersecurity threats. *IOP Conference Series: Materials Science and Engineering* 1226, (1). https://doi.org/10.1088/1757-899X/1226/1/012025.

van Daalen, O. (2022) In defense of offense: information security research under the right to science. *Computer Law & Security Review* 46 105706. https://doi.org/10.1016/j.clsr.2022.105706.

von Solms, B., and von Solms, R. (2018) Cybersecurity and information security – what goes where? *Information & Computer Security* 26, (1) 2–9. https://doi.org/10.1108/ICS-04-2017-0025.

von Solms, R., and van Niekerk, J. (2013) From information security to cyber security. *Computers & Security* 38 97–102. https://doi.org/10.1016/j.cose.2013.04.004.

Zeiringer, J. P., Durst, S., and Thalmann, S. (2022) Show Me What You Do and I Will Tell You Who You Are: A Cluster Typology of Supply Chain Risk Management in SMEs. *Journal of Theoretical and Applied Electronic Commerce Research* 17, (1) 345–359. https://doi.org/10.3390/jtaer17010018.

TAP Air Portugal (2023) A história da TAP. Disponível em: https://www.tapairportugal.com/pt/a-nossa-historia [Acesso em: 18 março 2023)

TAP Air Portugal (2023) Sobre a TAP. Disponível em: https://www.flytap.com/pt-pt/suporte/sobre-a-tap?=undefined [Acesso em: 18 março 2023]

TAP Air Portugal (2023) O Grupo TAP. Disponível em: https://www.tapairportugal.com/pt/sobre-nos/grupo-tap [Acesso em: 18 março 2023]

TAP Air Portugal (2023) Identidade TAP. Disponível em: https://recrutamento.tap.pt/go/Identidade-TAP/742202/ [Acesso em: 18 março 2023]

Anexos

Anexo I

Enquadramento Legal |
Decreto-Lei n.º 65/2021, de 30 de julho & Diretiva (EU) 2016/1148, de 6 de julho

Obrigação	Descrição	Legislação
Requisitos de segurança e de notificação	Cumprir quer os requisitos de segurança das redes e dos SIs, quer os requisitos de notificação de incidentes.	– DL nº 65/2021, art. 1º, nº 2.
Tratamento de dados pessoais	Aplicar rigorosamente o que está disposto na respetiva legislação.	– Diretiva (EU) 2016/1148, art. 2º; – Regulamento UE 2018/1725; – Regulamento EU 2016/679 (RGPD).
Ponto de contacto permanente	Indicar 1 ponto de contacto permanente e assegurar que tem uma disponibilidade contínua de 24/7.	– DL nº 65/2021, art. 4º, nºs 1 e 2.
Responsável máximo pela cibersegurança	Designar e indicar ao CNCS 1 responsável máximo pela Cibersegurança.	– DL nº 65/2021, art. 5º, nºs 1 e 4.
Inventário de ativos essenciais	Elaborar e manter atualizado um inventário de todos os ativos essencias para a prestação dos respetivos serviços.	– DL nº 65/2021, art. 6º, nºs 1 e 2.

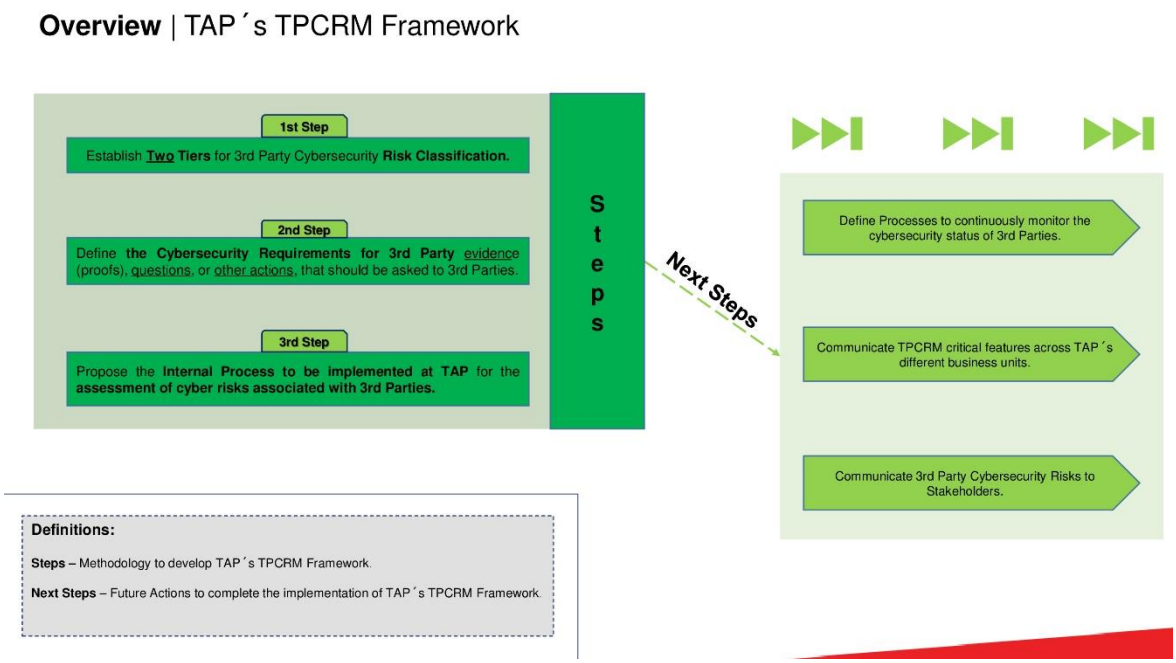
Anexo II

Enquadramento Legal |
Decreto-Lei n.º 65/2021, de 30 de julho & Diretiva (EU) 2016/1148, de 6 de julho

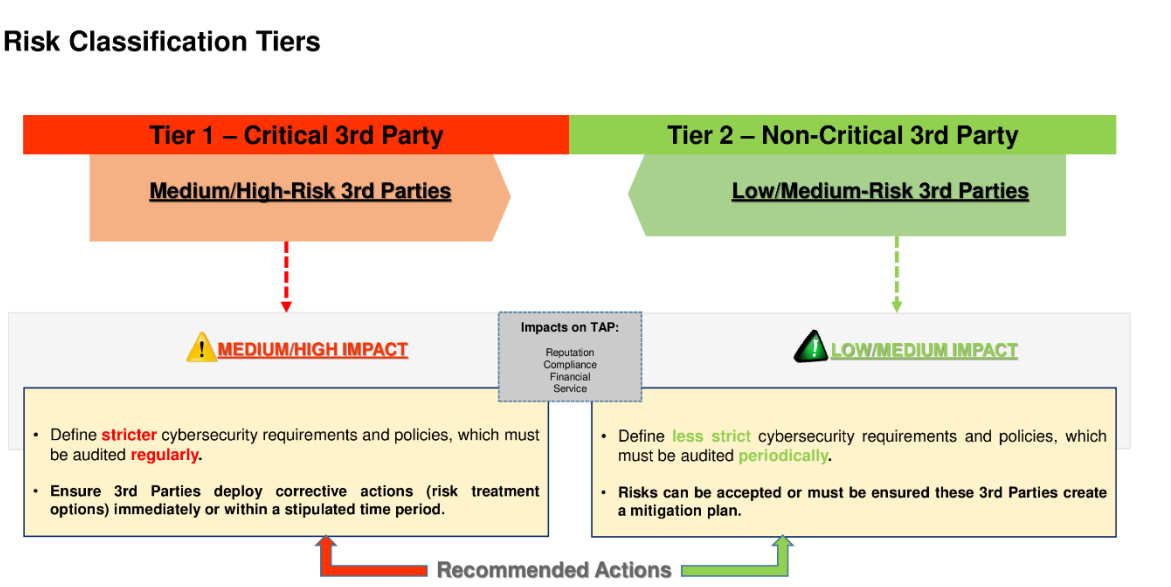
Obrigação	Descrição	Legislação
Plano de cibersegurança	Elaborar e manter atualizado um plano de cibersegurança.	– DL nº 65/2021, art. 7º, nº 1.
Relatório anual de cibersegurança	Elaborar um relatório anual de cibersegurança, que contenha os elementos referidos na respetiva legislação.	– DL nº 65/2021, art. 8º, nº 1.
Continuidade e Disponibilidade	Garantir que são tomadas medidas adequadas para evitar ciber incidentes que possam afetar a prestação dos seus serviços essenciais e digitais.	– Diretiva (EU) 2016/1148, art. 14º nº2 e art. 16º nº2.
Nível de cibersegurança	Implementar medidas de segurança que garantam um nível de cibersegurança, adequado ao risco em causa, tendo em conta os progressos técnicos + recentes.	– Diretiva (EU) 2016/1148, art. 16º, nº1.
Análise de riscos ampla e contínua	Cumprir medidas técnicas e organizativas para gerir os riscos de cibersegurança e realizar uma análise de risco ampla, atualizada periodicamente.	– DL nº 65/2021, art. 9º, nº 1.
Análise de riscos e ativos	Realizar uma análise de risco em relação a todos os ativos críticos.	– DL nº 65/2021, art. 10º, nº 1.

Obrigação	Descrição	Legislação
Documentação da análise de riscos	Realizar a documentação da preparação, execução e apresentação dos resultados da Análise de Risco; Identificar ameaças para cada ativo; Caracterizar o impacto e probabilidade de ocorrência de cada ameaça/risco.	– DL nº 65/2021, art. 10º, nºs 2 e 3.
Riscos residuais	Enquanto operador de infraestruturas críticas, deve tratar eventuais riscos residuais que possam surgir.	– DL nº 65/2021, art. 10º, nº 7.
Notificação de incidentes	Notificar o CNCS da ocorrência de qualquer incidente com impacto relevante ou substancial.	– DL nº 65/2021, art. 11º, nº 1.
Classificação de incidentes	Obrigatório classificar os incidentes como tendo impacto relevante ou substancial.	– DL nº 65/2021, art. 11º, nºs 2 e 3.
Tipos de notificações de incidentes	Submeter ao CNCS: uma notificação inicial, uma notificação de fim de impacto relevante ou substancial e uma notificação final. Caso o incidente seja resolvido nas primeiras duas horas, apenas é necessário submeter a notificação final.	– DL nº 65/2021, art. 12º, nº 1.
CSIRT	Obrigatório ter uma CSIRT e recomenda-se que esta esteja inserida na Rede Nacional de CSIRT.	– Diretiva (EU) 2016/1148, art. 9º nº2.

Anexo III



Anexo IV



Anexo V

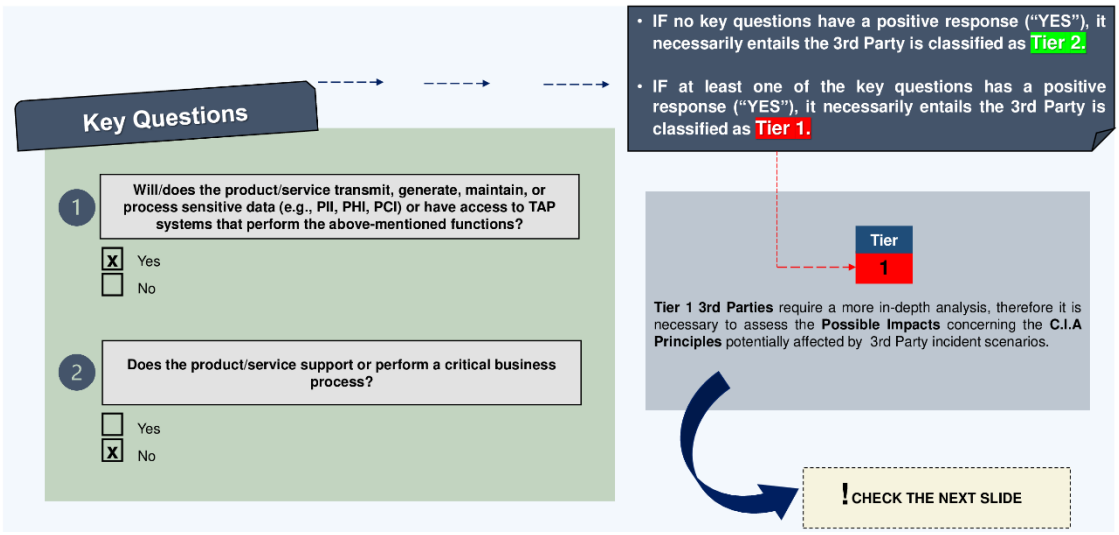
3rd Party Classification | Overview

3RD PARTY OVERVIEW:

"3rd. Party Name" --- **"Product/Service Name"**	- Website: 3rd Party Website **Point of Contact:** - Name: Name of 3rd Party Contact - Email: Email - Phone Number: Phone Number
TPCRMA Purpose and Objective	**Classify 3rd Party into Risk Classification Tiers**
Description of Service/Product and how is it used by TAP?	
Date of Assessment	**dd/mm/yyyy**
Assessor Name	**TAP´s Assessor Name**

Anexo VI

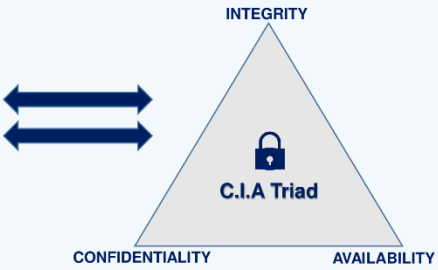
3rd Party Classification | Process



Anexo VII

3rd Party Classification | Tier 1 In-Depth Analysis

Impact level –>		1 Catastrophic	2 Major	3 Moderate	4 Minor	5 Insignificant
Impact Categories	Service	Unavailability of **mission critical systems.**	Unavailability of **business critical systems.**	Unavailability of a business critical system, or several **non-critical business systems** affecting a whole business process.	Unavailability of **non-critical business systems**, not affecting a whole business process.	No impact on service availability.
	Financial (under discussion)	?	?	?	?	No financial impact.
	Reputation	Ongoing focus of the Media in general.	One-off negative publicity in the Media or social networks in general.	Negative opinion limited to some Media or social networks.	Negative opinion limited to small groups, including in social networks.	No impact on reputation.
	Compliance (law/regulation, certification, contract)	General: Serious breach. May result in severe penalties, loss of certification, major contract termination. PII: Breach exposing sensitive personal data with risk of causing damage or distress to the affected individuals, or breach affecting a large amount of people.	General: Major breach. May result in significant penalties, damage to certification, non-major contract termination. PII: Breach exposing personal data with risk of causing damage or distress to the affected individuals, or breach affecting a substantial amount of people.	General: Moderate breach or probably infringement. Lack of good faith evident. May result in moderate penalties, or 3rd Party audits/reviews. PII: Breach exposing personal data with low risk of causing damage or distress to the affected individuals, or breach affecting a small amount of people.	General: Minor breach or complaint. Evidence of good faith arguable. May result in minor harm. PII: Breach exposing limited (in relevance) personal data, or affecting a few individuals.	General: Little or no compliance impact. PII: No personal data breach.



SPECIFICATION PROCESS:

Identify and Analyze the Potential Impact Categories affected by 3rd Party Incident Scenarios, and the matching Impact Level.
- Service
- Financial
- Reputation

Identify and Analyze Compliance Impact Separately (when 3rd party accesses, transmits, generates, maintains, or processes TAP PII).
- Compliance

Consider the C.I.A Triad and Identify the Principles affected by 3rd Party Incident Scenarios.
- Integrity
- Confidentiality
- Availability

Anexo VIII

3rd Party Classification | Template – **Tier 1**

"3rd. Party Name" ---------- "Product/Service Name"					
Impact Categories	Impact Level	MAX Impact Level	C.I.A		
			Integrity	Confidentiality	Availability
Service	1;2;3;4;5	1;2;3	X	X	X
Financial	1;2;3;4;5				
Reputation	1;2;3;4;5				
Compliance	1;2;3;4;5				

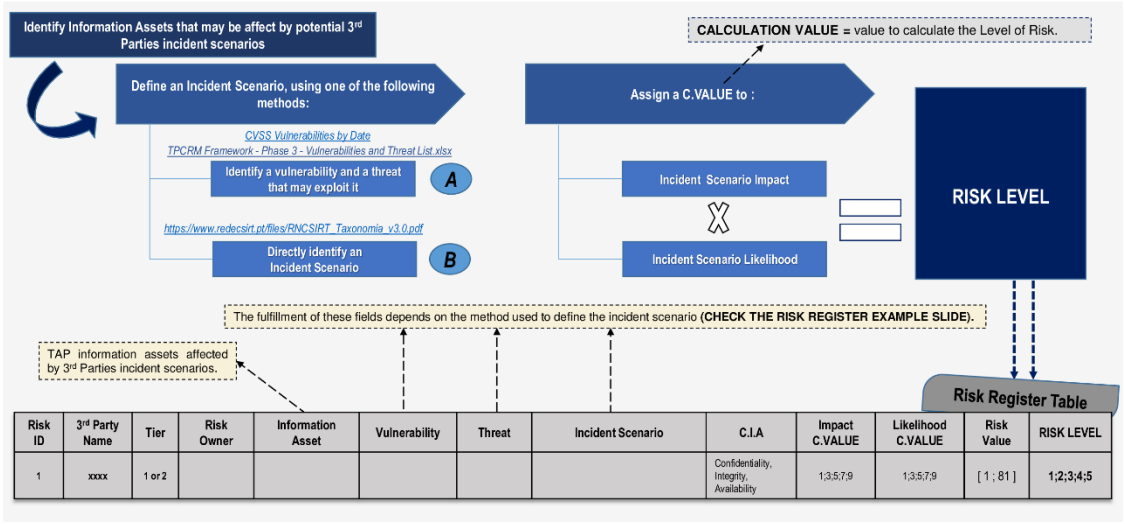
Specify the criticality (critical or non-critical) of the product/service delivered or the sensitivity of data (PII, PHI, PCI) accessed, transmitted, generated, maintained, or processed by 3rd Parties.

Examples:
- **3rd Party whose product/service has access, transmits, generates, maintains, or processes TAP`s PII (Personally Identifiable Information).**
- **3rd Party that delivers a critical product/service (ICT) to TAP.**

Key Notes:
- ! Mark with a "X" the C.I.A Principles affected by 3rd Party Incident Scenarios.
- ! Consider and propose enhancements to protect the C.I.A Principles which are essential to guarantee the protection of TAP´s information assets (includes PII).

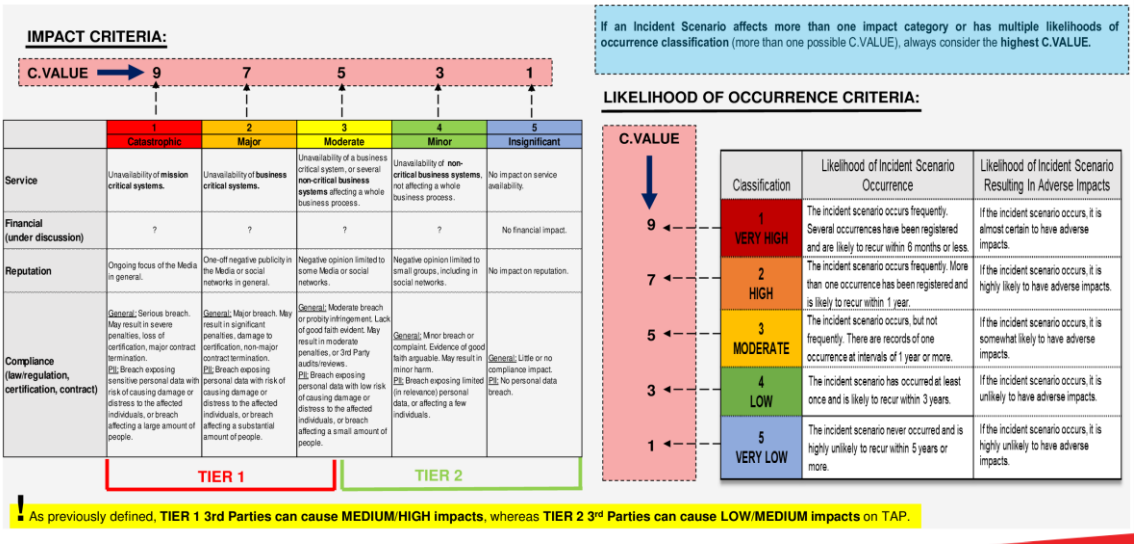
Anexo IX

Risk Analysis | Risk Analysis Process



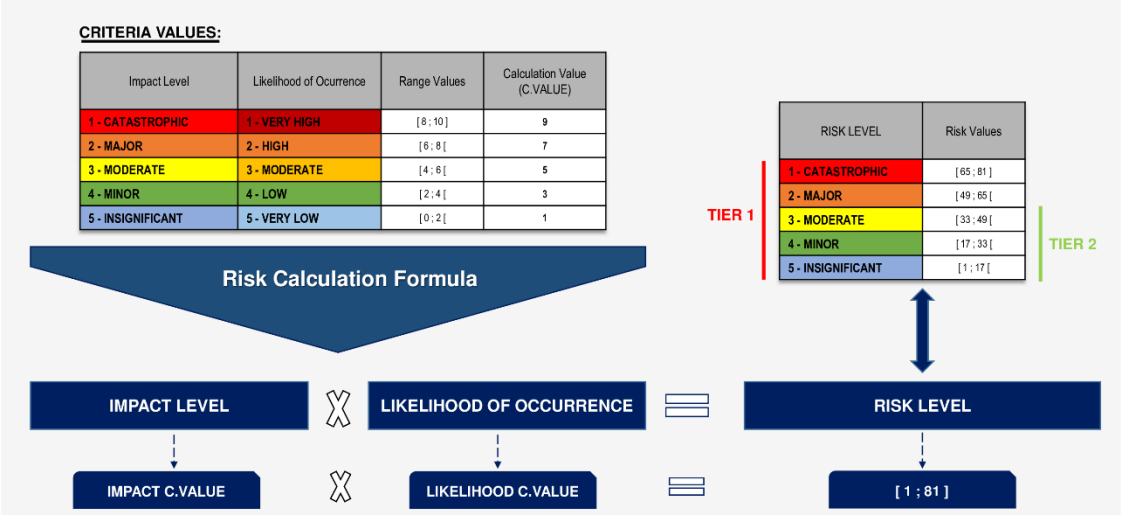
Anexo X

Risk Analysis | Impact and Likelihood of Occurrence Criteria (Incident Scenarios)



Anexo XI

Risk Analysis | Risk Level



Anexo XII

Risk Analysis | Risk Register Example