Susana Filipa da Silva Cardoso Dias

Consultoria em Gestão da Informação e Proteção de Dados: Estudo de caso da empresa Interaction Layer

Dissertação realizada no âmbito do Mestrado em Ciência da Informação, orientada pela Professora Doutora Olívia Manuela Marques Pestana e coorientada pelo Professor Doutor Bruno Reynaud de Sousa

Faculdade de Engenharia e Faculdade de Letras

Universidade do Porto

julho de 2020

Consultoria em Gestão da Informação e Proteção de Dados: Estudo de caso da empresa Interaction Layer

Susana Filipa da Silva Cardoso Dias

Dissertação realizada no âmbito do Mestrado em Ciência da Informação, orientada pela Professora Doutora Olívia Manuela Marques Pestana e coorientada pelo Professor Doutor Bruno Reynaud de Sousa

Membros do Júri

Presidente: Professor Doutor António Lucas Soares

Faculdade de Engenharia - Universidade do Porto

Orientadora: Professora Doutora Olívia Manuela Marques Pestana

Faculdade de Letras - Universidade do Porto

Arguente: Professora Doutora Maria Cristina Vieira de Freitas

Departamento de Filosofia, Comunicação e Informação - Universidade de Coimbra

“Para ser grande, sê inteiro:

Nada teu exagera ou exclui.

Sê todo em cada coisa.

Põe quanto és. No mínimo que fazes.”

Fernando Pessoa

Agradecimentos

A realização desta dissertação de mestrado é o culminar de uma importante etapa da minha vida e contou com apoios e incentivos fundamentais. Foram vários os que contribuíram para que fosse possível atingir o fim deste projeto, e deste modo desejo exprimir o meu mais sincero reconhecimento:

Aos meus Pais, com letra maiúscula, pela sólida presença e apoio incondicional, por me terem ensinado que a vida se faz de grandes conquistas, por trabalharem horas a fio e sem descanso para que conseguisse chegar onde cheguei. Nunca serão finitas as palavras de gratidão e reconhecimento por nunca me permitirem desistir daquilo que realmente importa, por sempre terem uma palavra de força para todos os momentos. Aos meus avós por estarem, constantemente, presentes neste percurso, por me ajudarem a alcançar mais um objetivo e pela incansável força e orgulho que sempre me transmitiram.

Ao meu irmão Pedro, pela inestimável amizade, generosidade, conselhos e incentivos para que este percurso académico fosse um sucesso. Sem vocês nenhuma conquista valeria a pena.

À Professora Doutora Olívia Pestana pela excelente orientação, pela motivação e constante disponibilidade de acompanhamento, que me depositou confiança em todo este processo, com sugestões e críticas que permitiram a melhoria contínua desta dissertação até ao seu estado final. Ao Professor Doutor Bruno Reynaud de Sousa, pela disponibilidade, sinceridade e pela partilha de informação que foi uma mais valia para o desenvolvimento deste projeto. Sem dúvida que sem o vosso auxílio não atingiria o trabalho que realizei.

Ao responsável Pedro Dias, CEO da empresa Interaction Layer, pela aprovação desta temática, oportunidade e por me proporcionar as melhores condições para esta concreção. Por toda a partilha de conhecimento, aprendizagem, disponibilidade, onde pude sempre contar com o apoio necessário para a concretização deste trabalho.

Ás minhas companheiras, Jéssica, Mariana Carvalho e Mariana Henriques, com quem partilhei os melhores anos académicos, agradeço a vossa energia contagiante que fez de vocês a minha luz em vários momentos, pela sinceridade e ajuda a integrar-me nesta

jornada, sempre de braços abertos. Amizades da qual levarei para a vida, que com a certeza de que o que vivi aqui não viverei em nenhum outro sítio.

Um agradecimento especial ao João, por nos momentos mais complicados se ter mantido a meu lado. Por acreditar em mim da forma mais verdadeira, por todo o apoio incansável e por toda a confiança e ânimo que me transmitiu.

Por último, agradeço a todos os professores que nestes dois anos me transmitiram de alguma forma motivação para continuar a trabalhar com esforço para atingir os meus objetivos e pela partilha de aprendizagem e conhecimentos adquiridos.

Ao meu avô paterno, que com carinho, dedico mais esta conquista.

A **todos**, um obrigada muito especial.

Resumo

Dada a importância da obtenção de certificação de qualidade, pretende-se, com esta dissertação, aprofundar conceitos associados à segurança da informação, bem como consolidar, na prática, as fases de implementação de um sistema de gestão, de modo a avaliar a aplicabilidade de uma norma. Desde o levantamento de ativos de informação até ao mapeamento dos fluxos de informação, foram efetuadas tarefas de implementação da norma ISO 27001, sendo esse o foco principal do trabalho.

Neste trabalho apresenta-se a análise e perceção da situação atual da empresa relativamente à consultoria das tecnologias de informação, para alcançar o conhecimento dos procedimentos e trazer contribuições para a melhoria destes processos. Será essencial, expor o novo regime de proteção de dados, através da aplicação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, estabelecendo a sua articulação com a norma de segurança a ser aplicada na empresa.

A determinação e a gestão de riscos são noções importantes na lei de proteção de dados e na normalização. A dissertação vem ao encontro de uma necessidade criada pelo artigo 25.º do regulamento geral da proteção de dados, na qual fundamenta dois princípios que as empresas são obrigadas a cumprir (proteção de dados desde a conceção e por defeito), tendo sido elaborado um manual de boas práticas.

Palavras-chave: segurança da informação, proteção de dados, ISO 27001.

Abstract

Given the importance of obtaining quality certification, it is intended, with this dissertation, to deepen concepts associated with information security, as well as to consolidate, in practice, the implementation phases of a management system, in order to evaluate the applicability of a standard. From the survey of information assets to the mapping of information flows, ISO 27001 implementation tasks were carried out, which is the main focus of the work.

This work presents the analysis and perception of the current situation of the company in relation to the consultancy of information technologies, in order to reach the knowledge of the procedures and to contribute to the improvement of these processes. It will be essential to expose the new data protection regime, through the application of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, establishing its articulation with the security standard to be applied in company.

Determination and risk management are important notions in data protection law and standardization. The dissertation meets a need created by article 25 of the general data protection regulation, in which it bases two principles that companies are obliged to comply with (data protection from conception and by default), having been elaborated a good practice manual.

Keywords: information security, data protection, ISO 27001.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

AD	*Active Directory (Software)*
APAV	*Associação Portuguesa de Apoio à Vítima*
BIOS	*Basic Input/Output System*
CE	*Comissão Europeia*
CRM	*Customer Relationship Management*
DPA	*Data protection authorities (Autoridades de proteção de dados)*
DPIA	*Avaliações de impacto na proteção de dados (Data protection impact assessments)*
DPbD	*Data Protection by Design (Proteção de Dados desde a Conceção)*
DPO	*Data Protection Officer (Encarregado de Proteção de Dados)*
EDPB	*European Data Protection Board*
ERP	*Enterprise Resource Planning*
FEUP	*Faculdade de Engenharia da Universidade do Porto*
IAF	*International Accreditation Forum*
IEC	*International Electrotechnical Commission*
IoT	*Internet of Things*
ISMS	*Information Security Management System*
ISO	*International Organization for Standardization*
NDA	*Acordo de Não-Divulgação (Non-Disclosure Agreement)*
PbD	*Privacidade desde a Conceção (Privacy by Design)*
Pbd	*Privacidade por defeito (Privacy by default)*
PDCA	*Plan - Do - Check – Act/Adjust*
RGPD	*Regulamento Geral da Proteção de Dados*
RH	*Recursos Humanos*

SGSI	*Sistema de Gestão de Segurança da Informação*
SI	*Sistemas de Informação*
SVN	*Apache Subversion*
TI	*Tecnologias de Informação*
TIC	*Tecnologias de Informação e Comunicação*
TPRM	*Third Party Risk Management*
UE	*União Europeia*
VPN	*Virtual Private Network*
VPS	*Virtual Private Server*

Glossário

Access Point – Dispositivo equiparado a um *router* sem fio, que permite que dispositivos sem fio se conectem a uma rede.
Disponível em: (https://techterms.com/definition/accesspoint) (Consultado em 03-06-2020)

Active Directory (AD) - é uma tecnologia da *Microsoft* usada para gerir computadores e outros dispositivos numa rede. É um recurso principal do *Windows Server*, um sistema que executa servidores locais e assentes na Internet.
Disponível em: (https://techterms.com/definition/active_directory) (Consultado em 03-06-2020)

BIOS – ("Sistema básico de entrada / saída"), é um programa pré-instalado em computadores baseados no *Windows,* que o computador usa para inicializar. A *CPU* acede à *BIOS* antes mesmo de o sistema operativo ser carregado. A *BIOS* verifica todas as suas conexões de hardware e localiza todos os seus dispositivos. Caso esteja tudo correto, a BIOS carrega o sistema operativo na memória do computador e finaliza o processo de inicialização.
Disponível em: (https://techterms.com/definition/bios) (Consultado em 03-06-2020)

CRM – ("Gestão de Relacionamento com Cliente"), refere-se à implementação de soluções, práticas, estratégias de negócio e tecnologias focadas no relacionamento com o cliente. Armazena informações de clientes atuais, atividades e pontos de contacto com a empresa entre outras interações. Capaz de reunir e integrar dados valiosos para preparar e atualizar as equipas com informações pessoais dos clientes, histórico e preferência de compras.
Disponível em: (https://techterms.com/definition/crm) (Consultado em 03-06-2020)

ERP – ("Planeamento de Recursos Empresariais"), é um software de gestão de processos de negócio que gere e integra as atividades, ações e recursos humanos de uma empresa (ex. finanças, ações de fornecimento, operações, relatórios, fabrico).
Disponível em: (https://dynamics.microsoft.com/pt-pt/erp/what-is-erp/) (Consultado em 03-06-2020)

LAN – ("Rede de área local"), é uma rede de dispositivos conectados que podem ser encontrados em instalações e áreas afins. Uma *LAN* pode ser feita por cablagem, sem fio ou uma combinação dos dois. Uma *LAN* com fio padrão usa Ethernet para conectar dispositivos juntos. A sem fio geralmente é criada usando um sinal Wi-Fi.

Disponível em: (https://techterms.com/definition/lan) (Consultado em 03-06-2020)

MAC Address – ("Endereço de controlo de acesso à mídia"), é um número de identificação de hardware que identifica exclusivamente cada dispositivo em uma rede. O endereço MAC é fabricado em todas as placas de rede, como uma placa Ethernet ou uma placa Wi-Fi.
Disponível em: (https://techterms.com/definition/macaddress) (Consultado em 03-06-2020)

ODOO – (anteriormente intitulado *OpenERP*), é uma solução de gestão empresarial ERP completo, com um sistema CRM. É baseado na arquitetura MVC (*Model-View-Controller*) e é realizada a comunicação entre o cliente e o servidor por interface XML. O Software é *open source* e disponível sob a *GNU General Public License*.
Disponível em: (https://pt.wikipedia.org/wiki/Odoo) (Consultado em 03-06-2020)

Pentesting – é um ataque cibernético simulado e autorizado a executar num sistema de um computador, realizado para avaliar a segurança do sistema. Usam estratégias e ferramentas projetadas para aceder ou explorar sistemas, redes, sites e aplicativos do computador. Embora também se possa usar ferramentas de teste, para testar a robustez das políticas de segurança de uma organização, a sua conformidade, a conscientização de segurança dos colaboradores e a capacidade de organização em identificar e responder a problemas e incidentes de segurança, como acesso não autorizado, à medida que ocorrem.
Disponível em: (https://www.contrastsecurity.com/knowledge-hub/glossary/penetration-testing) (Consultado em 03-06-2020)

Router - Dispositivo de hardware que roteia dados de uma rede local (LAN) para outra conexão de rede. Permite que apenas máquinas autorizadas se conectem a outros sistemas de computador. A maioria dos *routers* mantém arquivos de log sobre a atividade de rede local.
Disponível em: (https://techterms.com/definition/router) (Consultado em 03-06-2020)

Script-Kiddie – Considerados iniciantes de *hackers*, são indivíduos que não possui conhecimentos de programação e usa o software existente para iniciar um ataque. Muitas vezes, usam esses programas sem mesmo saber como funcionam ou o que fazem.
Disponível em: (https://www.uscybersecurity.net/script-kiddie/) (Consultado a 19/06/2020)

SVN - ("*Apache Subversion*"), é um sistema de controlo de versões e revisão de software distribuído como código-fonte aberto sob a Licença Apache. Programadores usam o *svn* para manter as versões atuais e biblioteca dos arquivos, como código fonte, páginas web e documentação.

Disponível em: (https://en.wikipedia.org/wiki/Apache_Subversion) (Consultado em 03-06-2020)

VPS – ("Servidor Privado Virtual"), é um servidor usado na virtualização de *software*. Funciona como um servidor físico, mas é uma instância virtualizada criada dentro de um servidor. Uma única máquina física pode hospedar vários servidores privados virtuais.
Disponível em: (https://techterms.com/definition/vps) (Consultado em 07-06-2020)

Frameworks - Plataforma para o desenvolvimento de aplicativos de software. Fornece uma base sobre a qual os desenvolvedores de software criam programas para uma plataforma específica (pode incluir classes e funções predefinidas). Programadores não precisam reinventar sempre que desenvolvem um novo aplicativo.
Disponível em: (https://techterms.com/definition/framework) (Consultado em 07-06-2020)

Sumário

1. Introdução

1.1. Contexto e motivação

A presente dissertação realiza-se na área de estudo da Ciência da Informação. Este tema enquadra-se na área referida, visto que a segurança da informação consiste num problema de gestão, e não somente de tecnologia. Neste sentido, a tecnologia encarrega-se em responder "a que ponto" será garantida a segurança da informação, enquanto a gestão pretende assumir o papel ao responder ao "que será feito" para garantir a segurança da informação (Zúquete 2008).

O Regulamento Geral de Proteção de Dados (RGPD), ilustra uma grande preocupação com dados pessoais de cariz sensível, que permite uma caracterização detalhada dos titulares dos dados, aumentando a abrangência de diversos tipos de dados.

A forma como as empresas se relacionam com os dados das entidades colaborativas ou de clientes, muda drasticamente com o RGPD, na medida em que as empresas enfrentam agora mudanças culturais e informáticas (Fonseca et al. 2018).

A introdução do RGPD no contexto europeu veio reforçar, a ideia que já existia antes. A ideia de que a matéria sobre a proteção de dados em todos os Estados-Membros, tem um papel cada vez mais importante no contexto jurídico-legal, e que necessitava de ser reformulada em alguns aspetos, dado todo o avanço tecnológico, no qual o titular de dados pessoais, terá a primazia sobre o seu direito fundamental à privacidade.

Quando se lida com informação sensível como aquela que se encontra ligada a organizações, as preocupações redobram-se, devendo os cuidados de segurança serem igualmente multiplicados.

De modo a estruturar e agir perante o desafio de abordar de modo organizado o tema de segurança da informação numa empresa focada na implementação de sistemas de informação, foram estudadas algumas das normas internacionais mais relevantes na área, bem como a legislação e regulamentação relacionada, em vigor no espaço jurídico em causa, abrangendo o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Nesse sentido, adotou-se para desenvolvimento do projeto a base da norma ISO/IEC 27001:2013.

Foi neste sentido que surgiu a ideia de desenvolver a presente dissertação intitulada "Consultoria em Gestão da Informação e Proteção de Dados: Estudo de caso da empresa

Interaction Layer", centrando-se na análise de um caso de estudo para avaliar a validade da norma ISO/IEC 27001:2013 para cumprir com a exigência da Proteção de Dados desde a sua Conceção do RGPD.

1.2. Enquadramento do projeto

1.2.1. Benefícios da solução a aplicar

As micros e pequenas empresas (MPEs) são vistas como os principais impulsionadores do crescimento económico, inovação, emprego e integração social. Representam 99% das empresas da União Europeia e empregam quase 50% dos trabalhadores da União Europeia.

Dado o papel significativo que as MPEs desempenham na sociedade e na economia da União Europeia, é aparente a importância de meios eficazes para evitar danos à segurança dos trabalhadores dessas empresas. Uma gestão eficaz de segurança nas PMEs é essencial para garantir o bem-estar dos trabalhadores, a sobrevivência e competitividade económica a longo prazo dessas empresas.

Nos últimos anos, as organizações têm sido alvo de mercados cada vez mais competitivos, onde a informação é o principal componente para a produção de conhecimento e formação de novas estratégias organizacionais.

A obtenção de certificações ou a atribuição de determinados carimbos de qualidade, torna as empresas mais competitivas e fortes, traduzindo uma vantagem competitiva para uma empresa. Atualmente, com o aumento da concorrência, as empresas necessitam de integrar diversos parâmetros diferenciadores para que consigam superar todas as dificuldades encontradas na área do mercado em que se inserem. Como tal, as obtenções de certificações de qualidade potenciam o aumento da competitividade através da satisfação das partes interessadas como colaboradores, fornecedores, clientes, e entidades do meio envolvente.

Conhecer aprofundadamente as normas de segurança que dominam um negócio é fundamental para sua manutenção e desenvolvimento. Porém, o incumprimento da regulamentação exigida na normalização, pode afetar uma empresa, capaz de impedir a certificação ou a atribuição de determinados carimbos de qualidade, tornando-a menos competitiva entre os concorrentes.

A estipulação de normas e medidas adotadas no RGPD é uma ação fundamental, o que permite às empresas serem mais competitivas, tornam-se referenciais para o mercado. As execuções das medidas normativas tornam o ambiente organizacional das empresas mais seguro, permitem estabelecer condições para a competição no mercado, além de facilitar a implementação de novas tecnologias que beneficiam na adoção das inovações.

Somente as empresas que adotam a regulamentação apresentam um exigente e expansivo mercado externo. A adoção das mesmas melhora a qualidade dos serviços concedidos pela empresa, associando valor à produção, e proporciona o aumento do rendimento, no qual pode ser aplicado na melhoria e no crescimento do negócio. Ademais, é capaz de garantir uma maior produtividade e rentabilidade, um melhor ambiente de trabalho e, consequentemente, um lucro mais elevado para o seu negócio. Diversas vezes ocorrem incidentes sem danos, mas que colhem consequências, perdas de tempo, eventualidades nos sistemas operativos, o que se compromete a credibilidade da empresa junto dos clientes, por deixar de cumprir a finalidade dos prazos estipulados.

1.2.2. Objetivos da dissertação e resultados esperados

Os objetivos que fundamentam a realização deste estudo são diversos. Contudo, aquele que se encontra na base de todos eles passam pela contribuição para uma melhor prestação na qualidade de serviços da empresa, que nos permitirá analisar a conformidade de acordo com a legislação e adoção das normas afetas às atividades da empresa.

Desta forma, será facilitado e verificado todo o processo da informação da empresa relativamente à segurança da informação, possibilitada para a melhoria do seu impacto na organização inerente, que significa uma notória evolução em comparação às empresas que desempenham funções e serviços no mesmo setor que a Interaction Layer atua.

Como referido na secção 1, esta dissertação tem como principal objetivo analisar um caso de estudo numa instituição de caracter de segurança informática, avaliar a validade da norma ISO/IEC 27001:2013 cumprindo com a exigência do artigo 25.º relativa à proteção de dados desde a sua Conceção e por defeito, afixada no Regulamento Geral da Proteção de Dados.

A fim de garantir que este objetivo seja alcançado, é fundamental que os objetivos específicos correspondam às suas necessidades como um todo. Com a existência de que são vários os objetivos do trabalho que advêm do objetivo principal, ou seja, que estes se encontram

ramificados ao objetivo de topo, ainda que uns contribuam para outros e cada qual tenha as suas próprias finalidades. Por conseguinte, para garantir que o objetivo principal, é necessário garantir a realização das tarefas intermédias e hierarquicamente inferiores, garantido que são executadas de acordo com o planeado.

No desdobrar do objetivo central estão dois grandes objetivos de segundo nível, com o intuito de poder melhorar e compreender o entendimento dos processos de negócio e a verificação do estado de auditoria.

A determinação e a gestão de riscos são noções importantes na lei da proteção de dados e a dissertação vem ao encontro de uma necessidade criada pelo artigo 25.º do regulamento geral da proteção de dados, na qual fundamenta dois princípios que as empresas são obrigadas a cumprir (proteção de dados desde a conceção e por defeito), e tal como a empresa não adquire essa concretização, será necessário a elaboração de um manual de boas práticas.

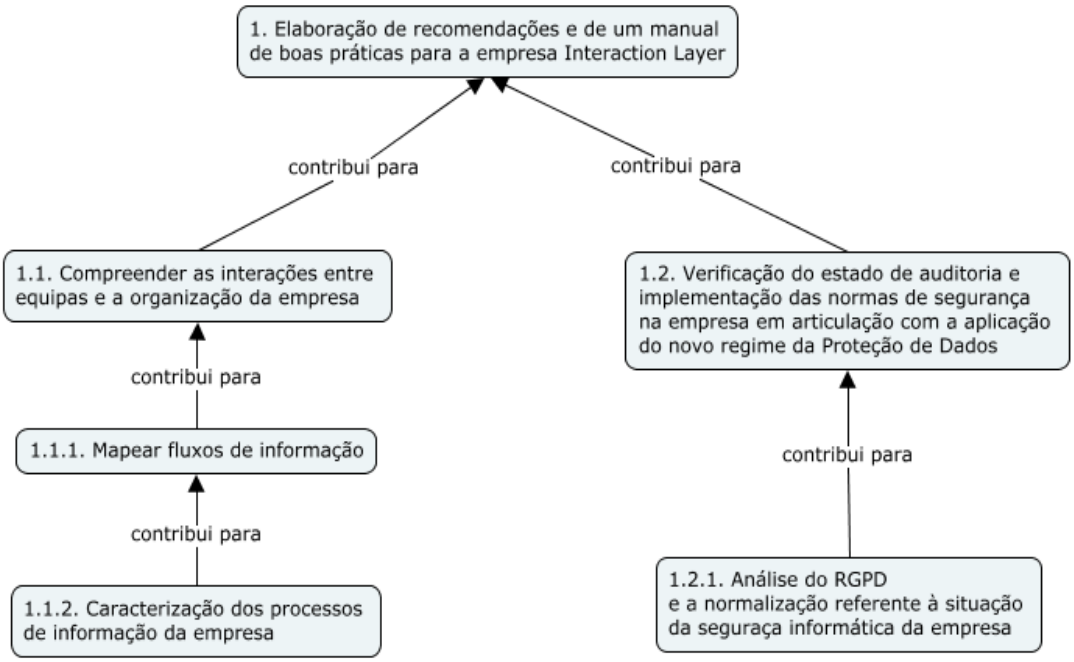


Figura 1 - Árvore de objetivos

Fonte: elaboração própria

1.2.3. Estrutura da dissertação

A fim de garantir uma estrutura organizada dos conteúdos abordados, a presente dissertação apresenta uma estrutura composta por cinco capítulos distintos, além da introdução, conclusão, referências bibliográficas e anexos.

Para que fosse possível entender o contexto do tema da presente dissertação foi necessária a realização de uma revisão de literatura minuciosa e extensa, devido à complexidade e termos não correntes do tema abordado. A mesma foi estruturada em três capítulos distintos, cada um deles diferenciados dos tópicos a abordar. Estes mesmos tópicos unem um conjunto de subtemas diretamente relacionados com o tema a desenvolver, permitindo realizar uma contextualização do mesmo, assim como entender a problemática em questão.

Na elaboração desta etapa inicial, procurou-se não só introduzir alguns conceitos essenciais para a compreensão da temática a abordar, como o Regulamento Geral da Proteção de Dados, o contexto normativo da ISO/IEC 27001 e o impacto que a lei tem nas organizações, mas também realizar uma conexão entre os mesmos, que permitisse compreender a necessidade do desenvolvimento do tema da dissertação.

Nesse sentido, no primeiro capítulo é abordada a questão da "segurança da informação organizacional", considerada um primeiro ponto essencial à luz do tema em questão. Visto que a dissertação envolve políticas e legislações associadas à segurança informática, faria de todo o sentido perceber a essência das práticas adotadas na atualidade nas empresas, onde referem exemplos de comuns incidentes de entidades corporativas, as dificuldades que demonstram em lidar com a segurança da informação e essencialmente demonstrar de que modo podem estar abertos para possíveis infrações ou ataques exteriores relativos a dados pessoais. Com o desenvolvimento destes subtemas pretende-se entender as ações concretizadas ao longo do tempo tanto por investigadores como a forma que as empresas se têm adaptado e implementado medidas organizacionais que demonstrem segurança a nível informático.

No segundo capítulo é abordado explicitamente o "Regulamento Geral da Proteção de Dados", que expõe a necessidade das empresas na adoção de leis e diretrizes capazes de tornarem as suas empresas mais seguras e certificadas com o regulamento geral da proteção de dados da União Europeia (UE). Refere-se todas as medidas necessárias para o controlo da informação e de dados pessoais com a finalidade de manter a segurança dos equipamentos e informações dos dados dos titulares, responsabilidades referentes ao encarregado da proteção de dados e ao controlador, com um grande e principal destaque nas diretrizes do artigo 25.º.

Posteriormente, no terceiro e quarto capítulo descreveu-se toda a informação referente às normas que auxiliam a garantir a segurança da informação numa organização. Como primeiro passo, foi fulcral aprofundar o conhecimento das normas que se pudessem aplicar à situação da empresa. Critérios impostos nesta temática forneceram ferramentas para avaliar a eficácia dos parâmetros de segurança, técnicas para a avaliação contínua da segurança e o controlo das violações de segurança e procedimentos para lidar com as respetivas falhas.

Refiro ainda que, no quarto capítulo foi necessário realizar um mapeamento da norma ISO/IEC 27001:2013 com o RGPD, na qual o regulamento em maior abrangência dispõe de detalhes suplementares que ajudam a estipular medidas e particularidades mais precisas. Tanto a norma como o regulamento, visam fortalecer a segurança dos dados e atenuar o risco das violações de dados, onde ambos exigem que as organizações garantam a confidencialidade, integridade e disponibilidade dos dados.

No quinto e último, é concretizado o estudo de caso onde, que após uma breve contextualização da instituição de estudo, serão apresentadas todas as análises ao estado de verificação da gestão de riscos e da auditoria realizada de acordo com a norma ISO/IEC 27001:2013.

As empresas mostram-se com dificuldades para lidar com a segurança da informação. Esses acontecimentos derivam do facto das organizações possuírem poucos mecanismos de proteção, intensificado pelo despreparo administrativo, tornando-as mais vulneráveis às ameaças e ataques. Estas análises e resultados do capítulo presente, servirão para um controlo e atualização do estado da empresa, no intuito de posteriormente plantarem melhorias com a ajuda de um manual de boas práticas, para garantir a proteção dos seus sistemas computacionais e ambientes organizativos. No entanto, nada prosseguirá caso o fator humano seja inalterável.

1.2.4. Abordagem metodológica

As abordagens metodológicas têm um forte impacto na perceção dos procedimentos a seguir face à recolha, tratamento, interpretação e difusão da informação relevante ao estudo, para alcançar os objetivos deste projeto de dissertação.

A abordagem metodológica adotada foi o método qualitativo de investigação, que se relaciona com a dimensão da investigação observacional e exploratória. Considerando que esta

dissertação abrange um caso de estudo numa instituição, torna-se evidente a necessidade da pesquisa exploratória para compreender o alvo a estudar.

O conhecimento sobre a articulação da norma ISO/IEC 27001 e o RGPD, (particularmente as medidas correlacionadas com a proteção de dados pessoais), está muito pouco estudado, com pouca informação visível, o que requer um foco no caracter exploratório para poder consagrar os objetivos aludidos.

Assim sendo, a primeira tarefa a ser realizada, que contribui de forma considerável para a abordagem metodológica, foi a elaboração de um esquema, (Figura 2), que organizasse de forma concisa as várias fases que complementariam esta dissertação e orientasse o percurso a seguir de forma metódica.

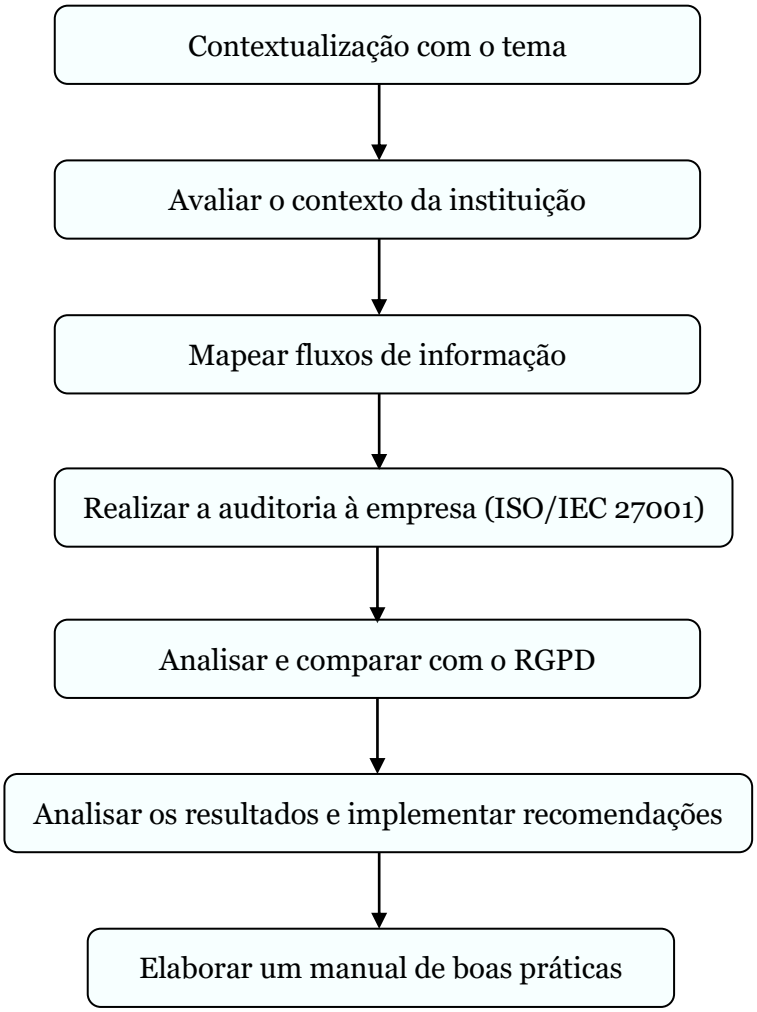


Figura 2 - Esquema com coordenação do trabalho

Fonte: elaboração própria

Primeiramente, foi necessária uma familiarização com o tema, definir as fontes bibliográficas para a recolha da revisão de literatura, e aprofundar o conhecimento das normas existentes, assim como do RGPD. Os principais termos usados como início à pesquisa foram "Normas de Segurança da Informação", "Normas de Segurança e RGPD" e posteriormente termos de pesquisa relacionadas com a "Norma ISO/IEC 27001" e "Artigo 25 do RGPD". Desta forma, foram selecionados critérios precisos como a seleção de documentos de língua estrangeira e materna e a exclusão de resultados sem relevância para o tema. No que se refere às fontes de informação usadas, pesquisou-se principalmente a *Elsevier (ScienceDirect, Scopus) e IEEE Xplore Digital Library,* consideradas as fontes relacionadas com temas de tecnologia e gestão da informação.

2. Segurança na gestão organizacional da informação

Nos últimos anos, as organizações têm sido alvo de mercados cada vez mais competitivos, onde a informação é o principal componente para a produção de conhecimento e formação de novas estratégias organizacionais.

Segundo Cruz (2012), a informação encontra-se nos ativos que envolvem uma organização, tendo um farto valor para o negócio, pelo que, a proteção da informação deve ser feita tendo em conta estes ativos.

Nesse contexto, Nakamura (2016), defende que os ativos da informação são compreendidos numa aglomeração que envolve indivíduos, tecnologia e processos, sendo os principais incumbidos em etapas no ciclo de vida da informação. Por sua vez, Sêmola (2014), delineia ativo como todo o componente que faz parte do processo de tratamento e modificação da informação, meios de armazenamento, equipamentos no qual são geridos e modificados.

Em conformidade, Cruz (2012), menciona os ativos como componentes físicos (arquivos, bibliotecas), tecnológicos (recursos informáticos, e-mails) e humanos (indivíduos que fazem parte das organizações).

Decorrente desta perspetiva, de acordo com Braga (2000), a Gestão da Informação faz "a ponte entre a gestão estratégica e a aplicação das Tecnologias de Informação (TI) nas empresas, procura, em primeiro lugar, tentar perceber qual a informação que interessa à empresa, para de seguida, definir processos, identificar fontes, modelar sistemas.", isto é, transmite a ideia de que é necessário existir uma interoperabilidade entre a informação, o conhecimento da organização e as TIC.

Neste sentido, a gestão da informação envolve, o conhecimento do ciclo de vida da informação até aos recursos tecnológicos, para que este processo seja implementado com sucesso numa organização.

> *"Managers of computer services have become information managers (and even directors of information management services), records managers, archivists, information scientists and special librarians have changed their titles and shifted their professional orientations, and educational institutions have introduced new courses in information management in departments as diverse as computer science, business management and librarianship."*
>
> (Feather and Sturges 2003)

De acordo com os autores Feather e Sturges (2003), existe uma relação que a Gestão da Informação tem com a Informática, estando cada vez mais presente nos vários sistemas informáticos nas empresas, devido à comum produção de informação em formato digital.

Por sua vez, a tecnologia torna-se uma porta aberta para a violação da informação. Os riscos da segurança da informação ameaçam a capacidade das organizações para atingir os seus objetivos operacionais e estratégicos. Milicevic and Goeken (2010), afirmam que "o aumento da diversificação dos padrões da segurança da informação torna-se uma adição a todos os riscos numa tarefa desafiadora", ainda que "os padrões de segurança da informação se posicionem como soluções genéricas para enfrentar uma ampla gama de riscos e tentar orientar os responsáveis da segurança nos seus empreendimentos" (Milicevic and Goeken 2010).

Em função desta realidade, as organizações têm vindo a procurar soluções, quer seja, "através da adoção de *frameworks* de gestão e da administração das TI já desenvolvidas e propostas pela comunidade profissional, ou então, por modelos próprios adaptados à realidade organizacional." (Bartens et al. 2014)

2.1. Princípios fundamentais e regularização dos dados pessoais

A secção anterior deixa clara a convicção da economia atual, na qual a informação é uma das razões prestigiadas nas organizações. Através dela, as empresas realizam a gestão dos seus produtos ou serviços, planeiam as suas estratégias, tornando desta forma os Sistemas de Informação (SI) ativos críticos, que requerem ser protegidos contra-ameaças que podem explorar as vulnerabilidades das infraestruturas. Estes danos na segurança causam a perda da confidencialidade, integridade e disponibilidade de informação, acarretando perdas financeiras por parte das empresas afetadas (Amaral, Amaral, and Nunes 2010).

Diversas organizações, sejam elas públicas ou privadas, ainda se mostram com dificuldades para lidar com a segurança da informação. Esses acontecimentos derivam do facto das organizações possuírem poucos mecanismos de proteção, intensificado pelo despreparo administrativo, tornando-as mais vulneráveis às ameaças. (Lunardi, Dolci, and Maçada 2010)

Num livro extremamente sugestivo, Whitman e Mattord (2018), referem que a segurança simboliza proteção. A proteção contra adversidades, quer para aqueles que causem danos de forma intencional ou não. Definem "Segurança da Informação" como a proteção da

informação e dos seus elementos críticos, incluindo os sistemas e *hardware* que usam, armazenam e transmitem as informações. Uma organização requer um sistema multifacetado, e para ser bem-sucedida deve ter várias camadas de segurança para proteger os seus procedimentos, infraestruturas físicas, pessoas, funções, falhas e informação.

De acordo com Weber (2010), torna-se fundamental garantir a segurança e a privacidade dos dados, através de conceitos dos processos de negócios, com um alto grau de idoneidade. Para esse fim, é significativo ter em conta requisitos como a resistência aos ataques direcionados a essas infraestruturas, na autenticação e na validação dos dados, no controlo de acessos e a privacidade do indivíduo.

Em conformidade, Bertino (2016), garante que a idoneidade, ou seja, a fiabilidade dos dados, exige um controlo rigoroso dos processos da gestão dos dados.

A segurança da informação é resultante de uma implementação de um agrupamento de medidas que envolve processos, tecnologias e pessoas. Permite proteger a informação, preservar o seu valor e garantir os princípios da disponibilidade, integridade, confidencialidade, autenticidade e a irretratabilidade ou não-repúdio (Ferreira 2017).

O autor ainda refere que, no que se vincula a essas características, as mesmas são mencionadas como atributos de uma segurança garantida, sendo a disponibilidade a "qualidade da informação estar sempre acessível e em condições autorizadas para o utilizador"; a integridade refere-se à "garantia de que a informação não foi alterada, sendo mantidas as suas características originais"; confidencialidade destaca-se pela sua propriedade que permite que a informação seja acedida apenas por utilizadores autorizados, evitando deste modo a propagação de conhecimentos e divulgações sem permissão. Sucede-se a autenticidade, que garante à informação ser encontrada na fonte originalmente anunciada. Quanto à irretratabilidade ou não-repúdio, concerne à não negação de ações referentes à informação como o seu envio, acesso, destruição ou modificação da mesma.

Conformemente ao que foi referido, Pimenta e Quaresma (2016), referem que os SI necessitam de estar sempre disponíveis, e para isso é crucial garantir a integridade e confidencialidade da informação que preservam e processam, além da tecnologia e de todos os mecanismos que se venham a adotar, um fator importante a ter em consideração são os utilizadores dos SI/TI.

2.2. Problemáticas associadas à privacidade da informação e regularização dos dados pessoais

Assimilados os efeitos da disseminação dos SI e das TI numa época tentada pelos dados e a maneira como estes se transformaram na sua proporcionalidade, de tal forma de como estes são recolhidos, acedidos, aplicados e modificados, é necessário conceber as problemáticas que estas se expõem relativamente à privacidade e proteção dos dados dos indivíduos.

A informação sensível, uma vez revelada ou divulgada, jamais poderá voltar a ser secreta, o que implica que o dano causado ao cidadão e o desrespeito pelo seu direito à privacidade nunca mais seja reposto (Yamamoto 2016). Neste âmbito, os direitos de privacidade e confidencialidade relacionam-se diretamente com o direito da proteção de dados pessoais.

Neste momento, é fulcral perceber o impacto das tecnologias no tratamento dos dados pessoais. Abordam-se respetivamente, perguntas frequentes como até que ponto os dados pessoais estão efetivamente seguros? As tecnologias inseridas em ambientes organizacionais tratam os dados devidamente? Os responsáveis pelo tratamento dos dados estão cientes das implicações das tecnologias de como estes dados são tratados?

A privacidade necessita de ser analisada desde o momento inicial, sob o ponto de vista tecnológico e desde a conceção dos SI que são desenvolvidos. Nesse sentido, Sousa, Pestana e Correia (2017), referem que as instituições organizacionais devem ter como prioridade a privacidade e proteção de dados de forma a não extraviar os dados. No entanto, a principal preocupação interliga-se essencialmente a questões relacionadas com a privacidade, sobretudo em dimensões na qual a informação pode ser associada ou ligada a um individuo em particular. E, fundamentando as tecnologias como suportes aos processos de recolha, armazenamento e tratamento de dados é imprescindível garantir a defesa dos direitos primordiais, levando em conta que o direto à privacidade assume novos desafios, à medida que as TI evoluem (Sousa, Pestana, and Correia 2017).

Os ativos da informação necessitam de ser esquematizados, devendo ser infringidos processos de mapeamento durante a planificação da segurança da informação, considerando que é de enorme importância a realização do grau de confidencialidade e de importância de acordo com a informação contida nos mesmos. Nesse contexto, os ativos independentemente do grau de confidencialidade e de importância, estão sujeitos a múltiplas vulnerabilidades que intervêm na segurança da informação.

2.2.1. Vulnerabilidades e sucessão de ameaças

Atualmente, testemunhamos uma crescente utilização de sistemas computacionais e recursos tecnológicos, o que vem dificultar a segurança ao acesso da informação e dos próprios sistemas que a armazenam, em particular, se o contexto descrito for organizacional. Diante disso, se a utilização íntegra de toda esta tecnologia concede para uma maior dinâmica de trabalho, então também provoca uma grande dimensão de complexidades que necessitam de serem pensadas para que estas não causem danos.

As vulnerabilidades estão presentes no dia-a-dia das organizações, apresentando-se nas mais diversas áreas. Identificar as vulnerabilidades e os impactos que podem causar nos negócios é fundamental para implantar medidas adequadas de segurança (G. L. de Oliveira 2017).

De acordo com Zúquete (2008), a vulnerabilidade é considerada "uma característica de um sistema que o torna frágil a certos ataques.". Nessa perspetiva e segundo Clinch (2009), considera-se que "uma fraqueza de um sistema é reconhecida por uma ameaça, como uma password nunca alterada".

No entanto, Sêmola (2014) conceitua vulnerabilidades como categorias de hardware, comunicação, físicas, software, naturais e humanas. Afirma ainda que estas se incluem presentes nos próprios ativos. Por si só, estas inseguranças não provocam eventualidades, porém são uma porta aberta para prejuízos, as ameaças.

Subsequentemente, T. R. Oliveira (2017), apud Peixoto (2006), refere que as vulnerabilidades categorizam-se como:

a) Naturais: danos naturais, (tempestades, incêndios, falta de energia, acúmulo de pó, aumento da humidade e temperatura) que podem causar anomalias aos computadores;

b) Físicas: salas de computadores mal organizadas e estruturas de segurança fora dos padrões exigidos;

c) Hardware: desgastes do equipamento ou má utilização;

d) Software: má instalação, erros de configuração ou fuga de informação;

e) Mídias: CDS podem ser perdidos ou danificados, e a radiação eletromagnética pode causar danos irreparáveis nos mídias;

f) Comunicação: perda de comunicação ou acessos não autorizados;

g) Humanas: falta de formações, consciencialização e o não cumprimento das políticas de segurança.

2.2.2. Análise de riscos e estratégias de defesa organizacionais

Um "risco", consiste na combinação da probabilidade de um evento ocorrer e as suas referentes consequências para a organização. Pode-se consumar que os riscos são a probabilidade de uma ameaça poder ser explorada através de uma determinada vulnerabilidade de um ativo de informação. As organizações devem minimizar os riscos até que estes deixem de o ser ou se tornem aceitáveis para as organizações (Coelho and Araújo 2013).

Um incidente é considerado um risco, caso afete a integridade, confidencialidade e disponibilidade de informação que os procedimentos vidam proteger. Nos dias que decorrem observamos o enorme número de ocorrências de ataques a organizações, na qual tende a aumentar ano após ano. Para Sudoski (2017), consideram-se como exemplo de incidentes os seguintes:

i) Acesso não autorizado às informações confidenciais, por agentes internos;

ii) Acesso não autorizado às informações internas, por agentes externos;

iii) Uso ou modificação não autorizada às informações confidenciais, por agentes internos;

iv) Uso ou modificação não autorizada às informações internas, por agentes externos;

v) Perda por circunstâncias ambientais (incêndios ou inundações);

vi) Falhas no sistema que acarretem ao acesso ou modificação não autorizada da informação.

vii) Roubo ou perda de informação por meio de transferência não autorizada (utilização de mídias removíveis para a transferência não autorizada das informações, ou transferência não autorizada em nuvem ou métodos online);

viii) Roubo de equipamentos *Bridge*[1] com armazenamento de informação;

Todavia, Coelho e Araújo (2013) especificam que a segurança da informação é apta a abranger todos os ativos de informação, preservando-os contra danos ou erros (intencionais ou não), tentando reduzir a probabilidade ou os impactos causados por incidentes de segurança.

Nessa perspetiva, Humphreys (2008), complementa que estes riscos são praticados pelos "*stakeholders*"[2] da organização, que aproveitam determinadas vulnerabilidades dos sistemas,

[1] Dispositivos que permitem interligar duas ou mais sub-redes e gerir de uma forma muito elementar, o tráfego entre as diferentes partes da rede. A bridge controla o tráfego das mensagens. Disponível em: (https://cefiredes1.webnode.pt/hardware/hardware-especifico/componentes-de-interliga%C3%A7%C3%A3o-de-redes/) (Consultado em 15-12-2019)

[2] Público estratégico e descreve uma pessoa ou grupo que tem interesse em uma empresa, negócio ou indústria, podendo ou não ter feito um investimento neles. Disponível em: (https://www.significados.com.br/stakeholder/) (Consultado em 15-12-2019)

processos e aplicações com inúmeras finalidades:

i) Ganho pessoal e lucro com o roubo de informação;

ii) Assumir um comportamento irresponsável (não ter intenção de causar danos);

iii) Danos mal-intencionados;

iv) Danos prejudiciais (ter a intenção de causar danos) a nível corporativo, operativo ou tecnológico" (Humphreys 2008).

Como solução apresentável, as organizações através da divulgação das respetivas normas, políticas e procedimentos de segurança da informação, relativamente a programas de consciencialização, saibam reconhecer e adotar as novas técnicas utilizadas e saber lidar com cada uma delas. Nesse sentido, as estratégias de defesa podem ser o recuso para garantir o nível de segurança.

De acordo com G. L. de Oliveira (2017), com a aplicação de procedimentos, fiscalizações, adoções de *firewall*[3] , filtros de conteúdo, deteção de pessoas não autorizadas (intrusos), testes de invasão (permitem a manutenção segura e preventiva em prol da segurança da informação), backup, e outras técnicas são aplicadas para atenuar as vulnerabilidades organizacionais, com objetivo de reduzir a viabilidade de ocorrência de ameaças e, por conseguinte, os incidentes de segurança da informação.

No momento em que há a aplicação de um ataque, é necessário identificar as restrições a serem implementadas, envolvendo um planeamento e uma atenção cuidadosa. As corporações utilizam diferentes práticas como auditorias de e-mails, gestão de relatórios de sites acedidos, avaliação comportamental e exploração do ambiente organizacional.

Entidades organizacionais estão expostas a áreas de risco de uma empresa, envolvidas em táticas comuns usadas pelos hackers, conforme a tabela 1. (Popper and Brignoli 2002)

[3] Dispositivo de segurança de rede que controla o tráfego de entrada e saída da rede e decide se deve permitir ou bloquear o tráfego específico com base num conjunto definido nas regras de segurança. Disponível em: (https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html) (Consultado em 29-11-2019)

Área de Risco	Tática do Hacker	Estratégia Adotada em Combate
Suporte informático	Representação e persuasão.	Desenvolver na empresa uma política de mudança de senhas e treinar os funcionários para nunca passarem senhas ou outra informação confidencial por telefone.
Entrada de edifícios	Acesso físico não autorizado.	Treinar os funcionários da segurança para não permitirem o acesso de pessoas sem o devido distintivo de identificação e mesmo assim fazer uma verificação visual.
Escritórios	1) Percorrer pelo ambiente; 2) Percorrer pelos corredores à procura de salas desprotegidas; 3) Roubar documentos importantes.	1) Não digitar senhas na presença de pessoas estranhas; 2) Todos os visitantes devem ser acompanhados por um funcionário da empresa; 3) Manter os documentos confidenciais fora do alcance de pessoas não autorizadas, de preferência em envelopes fechados, em locais seguros.
Suporte telefónico	Utilização de disfarces na hora de solicitar ajuda aos atendentes (geralmente passam-se por outras pessoas).	Os atendentes devem solicitar sempre um código de acesso, para só então prestarem o suporte solicitado.
Sala da correspondência	Inserção de mensagens falsas;	Fechar e monitorizar a sala de correspondência;
Sala dos servidores	Instalação de programas analisadores de protocolos para conseguirem informações confidenciais, além da remoção de equipamentos;	Manter sala dos servidores sempre trancada, e o inventário de equipamentos atualizado;
Central telefónica	Roubar acesso a linhas telefónicas;	Controlar chamadas para o exterior e para longas distâncias, e recusar pedidos de transferências suspeitas;
Depósito de lixo	Analisar o lixo;	Guardar o lixo da empresa num lugar seguro, triturar todo tipo de documento, e destruir todo o tipo de mídia magnética fora de uso;
Internet[4] e *intranet*[5]	Criação/inserção de programas na *internet* ou *intranet* para captura de senhas;	Criação de senhas fortes e utilização consciente da mesma, alterando-a periodicamente. Os *modens*[6] nunca devem ter acesso à *intranet* da empresa;

Tabela 1 - Áreas de Risco, Táticas e Estratégias

Fonte: Popper and Brignoli (2002)

Decorrente desta referida iniciativa, a importância das TI expandiu-se ao longo dos anos e com o seu aproveitamento implicou-se alterações bastante pertinentes. O RGPD, neste sentido, representa uma forma de sensibilizar as organizações quanto à necessidade de garantir a segurança da informação, padronizar o ciclo de vida dos dados e evitar deste modo a sua utilização excessiva.

2.2.3. Programas e ações de consciencialização

As entidades corporativas realizam grandes investimentos na tecnologia, para garantir a proteção dos seus sistemas computacionais e ambientes organizativos. No entanto, nada prosseguirá caso o fator humano seja deixado posterior ao primeiro plano (G. L. de Oliveira 2017). Dado esse princípio é fundamental a consciencialização, ou contrariamente a organização corre enormes riscos, dado que as vulnerabilidades humanas são percetíveis e exploradas. A adoção de programas e formações "tem um objetivo muito mais significante que simplesmente impor as regras" (G. L. de Oliveira 2017).

Nesse caso, os utilizadores devem ser advertidos para questões de segurança, nomeadamente para que exemplos de consequências uma dada violação de segurança poderia provocar (Kruger and Kearney 2008). Portanto, será fulcral a adaptação de boas práticas e medidas de segurança para garantir um comportamento natural dos utilizadores dentro de uma organização.

No entanto, as organizações, além de necessitarem adotar medidas e normas de segurança dos SI, devem também motivar os utilizadores a aplicá-las, elaborando paradigmas de simulações, para não prejudicar as ações na qual poderão provocar vulnerabilidades nas organizações e, consequentemente, ataques aos SI (Workman, Bommer, and Straub 2008). Sendo que o objetivo de um programa de consciencialização sobre a segurança da informação é influir aos funcionários a transmutar os seus comportamentos e atitudes, seria eventualmente mais vantajoso motivar cada trabalhador a cumprir a sua parte relativamente à proteção dos ativos de informação na organização.

[4] Rede que conecta computadores a nível global. Conjunto de protocolos específicos utilizados para conectar utilizadores.

[5] Conecta computadores a um nível bastante específico, sendo este o motivo de ser utilizado como uma ferramenta de comunicação interna nas empresas. Oferece mais segurança por ser uma rede fechada. Disponível em: (http://www.postdigital.cc/blog/artigo/qual-a-diferenca-entre-intranet-e-internet) (Consultado em 28-11-2019)

[6] Dispositivo eletrônico que modula um sinal digital numa onda analógica, pronta a ser transmitida pela linha telefônica. Disponível em: (https://www.palpitedigital.com/o-que-e-um-modem/) (Consultado em 28-12-2019)

Apesar desta notória evolução, torna-se num processo aliciante divulgar pela empresa, através de comunicados internos, documentos online e casos fracassados no que tange à quebra da segurança (Mitnick and Simon 2005). O autor, evidencia ainda, o uso de métodos rigorosos de autenticação sem serem fornecidos por senhas estáticas, o estabelecimento de uma política de segurança corporativa, o reforço de todos os sistemas relacionados com o cliente que acede a informação sigilosa ou a recursos informáticos, o uso de dispositivos de deteção e de intrusão. Imprescindível será para uma organização que se queira tornar segura, a ativação de recursos de auditoria dos sistemas operativos e aplicativos críticos.

3. O Regulamento Geral da Proteção de Dados

3.1. Âmbito material e âmbito territorial

O Regulamento Geral da Proteção de Dados[7] (RGPD), contém um conceito amplo referente a dados pessoais. Nos termos do artigo 4.º, n.º1 dados pessoais é a "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;" (cf. artigo 4.º, n.º1, do RGPD).

Neste contexto, definir dados pessoais de dados não pessoais, é um elemento primordial, e caso uma entidade processe dados, esta está sujeita às várias obrigações que o regulamento impõe, nomeadamente os controladores de dados.

Segundo Finck e Pallas (2019), dados pessoais são informações ou conjunto de informações distintas que se referem a uma pessoa viva, identificável. Ainda que estes dados possam ser pseudonimizados ou codificados, mas que possam continuar a ser utilizados para reidentificar um individuo, continuam a ser dados abrangidos pelo regulamento.

O autor refere ainda que, de acordo com o regulamento, dados pessoais que tenham sido transformados em dados anónimos (de forma a que deixem de identificar um individuo), estes deixam de ser categorizados como dados pessoais, de modo que o seu vínculo com a pessoa identificável tenha sido removido.

Substancialmente, o RGPD concebeu um modelo que obriga as entidades organizacionais a considerarem questões relacionadas com a proteção de dados e as ameaças de privacidade dos dados pessoais. Para esse efeito, foi necessária a reformulação e definição de conceitos, assim como obrigações associadas.

Resultam diversas inovações, nomeadamente:

a) A introdução de um conceito de "violação de dados pessoais"; (cf. artigo 3.º, do RGPD)

[7] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Consultado em 22-12-2019)

b) A introdução de novos princípios e conceitos que devem nortear o tratamento dos dados como a proteção de dados desde a sua conceção e por defeito, ou a pseudonimização dos dados; (cf. artigo 25.º, do RGPD)
c) O direito a ser esquecido; (cf. artigo 17.º, do RGPD)
d) O direito à portabilidade dos dados; (cf. artigo 20.º, do RGPD)
e) A figura do encarregado de proteção de dados; (cf. artigos 37 a 39.º, do RGPD)

De facto, procurou-se a averiguação de "regimes jurídicos no contexto da UE", como estabelecer legislações em domínios importantes que não se encontram devidamente protegidos, ou acompanhar a evolução tecnológica que, por defeito, está em constante mutação (Ramos 2016). Estas determinações aferiram a atualização do regime jurídico da proteção de dados, com uma perspetiva e precaução das bases tecnológicas, assim como a necessidade da existência de um regulamento para o futuro.

Segundo o RGPD da União Europeia, aprovado a 27 de abril de 2016, entrou em vigor a 25 de maio de 2018, constitui uma reforma à Diretiva de 95/46/CE, "relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", que estabelece regras para o tratamento, armazenamento e gestão de dados pessoais que estão atualmente dentro da União Europeia.

De acordo com Carvalho e Antunes (2018), a inevitabilidade sobre a crescente proteção da privacidade dos indivíduos e dos seus dados pessoais, é de todo um ato fulcral. Identicamente, o direito à informação criou uma conexão com a privacidade. Os autores afirmam que, atualmente, o direito à informação engloba um discernimento mais completo da proteção de dados, no qual se destaca o acesso aos dados por parte do individuo, bem como o direito às decisões, seja a nível público ou privado.

Neste sentido, o Conselho Europeu para a Proteção de Dados[8] (2019), refere que o presente regulamento impõe a rigorosa aplicação das boas práticas de segurança e privacidade dos dados, seja o consentimento informado, a pseudonimização, a encriptação ou anonimização de dados, a notificação de violação de privacidade, nomeação de "responsáveis" por dados pessoais nas empresas, entre outras, na qual, a obrigação às mesmas requerem à aplicação de reformas significativas nos processos e sistemas organizacionais, perante a pena de acentuadas coimas e penalizações (cf. artigo 84.º, do RGPD).

[8] Conselho Europeu para a Proteção de Dados (EDPB)

No que diz respeito à aplicação territorial do regulamento, este aplica-se exclusivamente ao tratamento de dados pessoais de titulares residentes no território da UE, seja o responsável pelo tratamento dos dados situado em mesmo território, ou um responsável situado exterior à UE, mas que eventualmente realize tratamentos de dados pessoais incidentes sobre pessoas singulares que pertençam à UE.[9]

3.2. Obrigações que decorrem para as organizações

A considerada secção formula necessidades que devem ser adotadas nas organizações para que as mesmas estejam em conformidade com o regulamento, e de que forma é que estas incumbências se conformam com a segurança da informação.

Nos termos do artigo 37.º, existem determinados responsáveis pelo tratamento de dados, alguns dos mesmos são obrigados a designar um Encarregado da Proteção de Dados (*DPO*).

O artigo 37.º, especifica que uma organização deve intitular um responsável da proteção de dados sempre que o tratamento de dados for realizado por um organismo público, com exceção de tribunais e exercícios de deveres jurídicos. É dever dos encarregados, a execução de atividades com base organizacional que consistam no controlo regular e sistemático dos dados em grande escala (cf. artigo 37.º, n. º1, do RGPD).

Designa-se então por *DPO*, o responsável pela coerência com o regulamento de uma dada organização. Porém, é importante referir que o papel do responsável também auxilia como intermediário aos titulares dos dados e à entidade reguladora.

Com efeitos no artigo 24.º, a "Responsabilidade do responsável pelo tratamento", refere que a organização deve ter documentada toda a informação relativa a políticas e procedimentos que comprovem a conformidade da organização com o regulamento (cf. artigo 24.º, n. º1, do RGPD).

Nos termos do artigo 25.º, está circunstanciado o dever de as organizações necessitarem de incorporar a proteção de dados apropriada desde a sua conceção e por defeito, no decorrer do desenvolvimento dos processos, levando fulcralmente em conta características como os dados que tratam, o gênero de tratamento, os riscos que acarretam, de forma a estarem em

[9] Conceitos presentes na seção são fundamentados no Regulamento Geral de Proteção de Dados da União Europeia, 2016. Consultado em 22-12-2019

conformidade com o regulamento, e essencialmente proteger os direitos dos indivíduos. Contudo, devem ser aplicadas medidas de forma a garantir apenas a recolha dos dados necessários, processados e acedidos até o mesmo deixar de ser útil para a finalidade recolhida (cf. artigo 25.º, n.º 1, do RGPD).

Nas definições do RGPD, as "Condições aplicáveis ao consentimento", ao que o nome indica, dados processados deverão ser baseados no consentimento. A organização deve ser capaz de comprovar que a entidade revelou permissão para tal. A mesma deverá esclarecer a finalidade para qual os dados são recolhidos, e deve ser permitido voltar atrás na decisão do consentimento dos indivíduos (cf. artigo 7.º, n.º 1, 3 e 4, do RGPD).

De acordo com Boardman, Mullock e Mole (2019), existem diversos aspetos relacionados com a aplicabilidade do consentimento dos titulares dos dados (incluindo toda a sociedade da informação), como a clarificação do tratamento legitimo dos dados, finalidade, interesses dos responsáveis pelo tratamento dos dados aos direitos e liberdades dos titulares dos dados e a inclusão de novos tipos de dados no tratamento de dados sensíveis, dados genéticos, biométricos e de saúde (Boardman, Mullock, and Mole 2019).

Segundo o artigo 33.º, a secção referente "Notificação de uma violação de dados pessoais à autoridade de controlo", define que, caso haja uma fuga de informação a nível de dados pessoais, a organização num período de 72 horas deverá notificar a entidade reguladora, informando eventuais danos, o número de cidadãos afetados e possivelmente o contacto do Encarregado de Proteção de dados para uma aquisição de detalhes mais aprofundados (cf. artigo 33.º, n.º 1, 2 e 3, do RGPD).

O RGPD não define explicitamente o que é um país terceiro. Na perspetiva do âmbito territorial na aplicação do RPGD, todos as decisões são realizadas por referência à UE. Conforme o artigo 44.º, designado como "Principio geral das transferências", obriga as organizações caso haja transferência de informação através das fronteiras, a garantirem por parte de terceiros o cumprimento com o regulamento, e essencialmente, apresentar as razões devidamente justificadas que levaram à execução do ato (cf. artigo 44.º, do RGPD).

No âmbito da presente tese, cumpro esclarecer que a empresa Interaction Layer, é obrigada a nomear um *DPO*, função encarregada de controlar a empresa na toma das decisões referentes ao tratamento de dados pessoais dos titulares, para que se tenha uma política de tratamento transparente e correta. Independentemente do mesmo ser uma entidade interna ou externa, é crucial a sua execução de ações, na qual, coordenará e orientará a empresa, nas normas de

proteção de dados e na implementação de melhores práticas para a mesma. Além de ser um contacto responsável pela notificação de uma violação com as autoridades de controlo.

Deste conjunto de necessidades, a empresa deste caso de estudo, tem por obrigação não só a nomeação de um *DPO*, como também cumprir com o princípio geral de transferência caso exerça ações para países terceiros.

O regulamento estabelece determinadas responsabilidades às organizações, na garantia da preservação dos dados por tempo necessário, de forma a incutir a sua utilização exclusivamente na finalidade para o qual foram recolhidos, e claro que, os mesmos necessitam de continuar a serem protegidos, isto, através da implementação de medidas de segurança da informação (Fonseca et al. 2018).

Cuesta (2018), destaca que as funções dos gestores de informação são extremamente relevantes para a realização de determinadas tarefas, como na arquitetura de sistemas da gestão de informação, na decisão dos documentos a serem definidos e recolhidos, bem como o tempo que devem ser preservados. Estes profissionais são, também, fundamentais para definir e delinear os requisitos da sua gestão, como também por quanto tempo será necessário conservá-los.

Evidencia-se uma abordagem integrada, que permite implementar e cumprir o regulamento de forma eficiente e eficaz, em áreas como a Gestão de Informação, Direito e Segurança da Informação, na qual o *DPO*, deve ser qualificado com base em qualidades profissionais, no domínio do direito e das práticas de proteção de dados (Fonseca et al. 2018).

No entanto, Fonseca afirma que o profissional de informação é um elemento privilegiado neste contexto, dado que possui competências eminentes e relevantes no que toca ao tratamento da informação e que ampara na aplicação do RGPD em serviços da gestão de informação e arquivologia, na qual se equipara ao "equilíbrio entre a proteção dos interesses das pessoas e a proteção da liberdade de informação" (Fonseca et al. 2018)

Na área da Ciência da Informação, é crucial assegurar a integridade e autenticidade dos documentos, preservando-os a longo prazo, sem eliminações parciais, capazes de garantir a proteção dos direitos dos cidadãos e dos seus ascendentes, bem como o valor comprovador dos documentos (Fonseca et al. 2018).

3.3. Impacto para os responsáveis de tratamento de dados

O RGPD, tem como objetivo a uniformização da execução e aplicação da legislação no que refere ao tratamento de dados pessoais, garante a segurança jurídica e a atividade económica, sem entraves e uma livre concorrência (Fonseca et al. 2018).

De acordo com Batalha (2017), o regulamento já é atualmente considerado uma complicação significativa que influenciou a grandes mudanças e impactos nos negócios, e como este é considerado uma regulamentação que para além de ter de ser cumprida de igual forma em todos os países da União Europeia, a sua implementação é obrigatória nos considerados países de Estados-Membros.

Embora, os dados pessoais, os grandes volumes de dados e a computação em *cloud*[10] sejam cada vez mais requisitados e utilizados pelas empresas, no intuito de fundamentar decisões de gestão, denota-se que os princípios sobre a proteção de dados e privacidade dos trabalhadores são quase inexistentes.

Em simultâneo, o responsável pelo tratamento deve, no momento da determinação dos meios de tratamento, implementar medidas técnicas e organizacionais apropriadas, como a pseudonimização, projetadas para implementar princípios de proteção de dados (como a minimização de dados). Com o objetivo de ser eficaz nas salvaguardas necessárias ao tratamento, a fim de cumprir os requisitos do regulamento e proteger os direitos dos titulares dos dados (Veale, Binns, and Ausloos 2018). Pra além dos encargos anteriores, o responsável pelo tratamento deve implementar medidas adequadas para garantir que os tratamentos de dados sejam apenas necessários para a finalidade do qual foram recolhidos, para que os dados pessoais não sejam acessíveis sem a intervenção do individuo a um número indefinido de pessoas físicas.

Essencialmente, o regulamento vem adotar um modelo que obriga as organizações e entidades a considerarem questões relacionadas com a proteção e os riscos da privacidade dos dados pessoais. Nesse sentido, as organizações devem obter o consentimento do utilizador para a recolha dos dados e "implementar medidas técnicas e organizacionais apropriadas", para proteger os dados pessoais dos residentes da União Europeia (Li, Yu, and He 2019).

[10] Fornecer serviços informáticos, incluindo servidores, armazenamento, bases de dados, rede, software e análises através da Internet. (https://azure.microsoft.com/pt-pt/overview/what-is-cloud-computing/) Consultado em 31-01-2020

Adotar a implementação dessas práticas para a minimização das informações que terceiros poderão aceder é cada vez mais um assunto popular entre produtores de software e hardware. Empresas de nome conceituado (*Apple*), incluem dispositivos com endereços randomizados, que impedem tipos de ataques de segurança, tornando-os mais difíceis para um atacante para prever endereços de destino. De forma similar, para dificultar o rastreamento, normalmente utiliza-se uma transformação unidirecional de dados (função *hash*), que se baseia na adição de *strings*[11] à informação dos dados (Finck and Pallas 2019).

Uma outra disposição que está referenciada no RGPD é o "Direito de oposição", no qual os titulares de dados pessoais devem ter o direito de se oporem ao tratamento de quaisquer dados pessoais (cf. artigo 21.º, do RGPD), a menos que o responsável pelo tratamento possa demonstrar que o seu interesse legítimo substitui os interesses/direitos/liberdades fundamentais que digam respeito à situação específica (cf. considerando 69, do RGPD).

A implementação do RGPD (particularmente a nível de dados pessoais), veio transformar de uma forma significativa a proteção nas organizações. Desta forma, o objetivo principal, não é o de beneficiar a adoção de ferramentas que permitem a proteção nas organizações, mas o de garantir a integridade da proteção de qualquer titular de dados pessoais.

Proclama-se às empresas, o lançamento de novos desafios e regras relativas à proteção de dados pessoais. Moreira (2018) refere que, o regulamento apresenta objetivos primordiais como "implementar nos Estados-Membros mecanismos legislativos aliados à contínua evolução tecnológica, aumentar a proteção dada a todos os titulares de dados pessoais às ameaças e a utilização indevida desses dados pelas organizações, além de complementar a iniciativa da UE relativamente ao Mercado Único Digital[12], no que promete ser um novo mecanismo de oportunidades para todos os cidadãos europeus e Estados-Membros, desde que disponham das competências digitais necessárias."

Sendo este regulamento, capaz de fortalecer a proteção de dados da UE para enfrentar os novos desafios de privacidade (abordados pelo desenvolvimento das tecnologias digitais), tornou-se o mais severo do mundo. Redigida e aprovada pela UE, "impõe obrigações às organizações em

[11] Na programação de computadores, uma cadeia de caracteres ou *string* é uma sequência de caracteres, geralmente utilizada para representar palavras, frases ou textos de um programa

[12] Estratégia da CE para assegurar o acesso a atividades online para indivíduos e empresas em condições de concorrência, proteção dos consumidores e dados, eliminando problemas de direitos autorais. Disponível em: (http://business.turismodeportugal.pt/pt/Conhecer/Oportunidades_UE/programas-iniciativas/Paginas/digital-single-market.aspx) (Consultado em 31-01-2020)

qualquer lugar, desde que elas tenham como alvo ou se associem a dados relacionados com pessoas na UE".

De acordo com Nurse, Creese e Roure (2017), nos últimos anos, a proteção de dados tornou-se uma questão de vanguarda na cibersegurança. Pormenorizam ainda que, "os problemas introduzidos por violações recorrentes de dados organizacionais, mídia social e a *Internet of Things (IoT),* aumentaram ainda mais os riscos". No âmbito do tópico destacado na dissertação, devido ao modelo de negócio que a empresa Interaction Layer tem, o principal impacto é do artigo 25.º do RGPD.

Atualmente, a principal fonte de comunicação que é partilhada de humano para humano é a Internet. A posterior forma de comunicação que usa a Internet como tecnologia subjacente é a *IoT*, que amplia os recursos da Internet para permitir a comunicação "máquina-a-máquina". Esta fonte de comunicação permite incorporar alguma inteligência nos objetos que são conectados à Internet, a fim de trocar informações, comunicar, invocar ações, tomar decisões e fornecer serviços úteis. Hoje, a *IoT* está a ganhar um forte reconhecimento devido ao seu potencial, ainda a ser desenvolvido pelas indústrias e instituições organizacionais. Setores como esses poderão eventualmente trazer benefícios econômicos e profissionais, recorrendo à IoT da maneira mais correta. (Chopra, Gupta, and Lambora 2019).

3.4. O impacto nas empresas: caso especial do artigo 25.º

No âmbito desta dissertação, surge a pergunta que tanto se mitiga "Porque razão as empresas se devem preocupar com o RGPD?" Primeiramente retrata dados pessoais e tem um conceito amplo, segundo porque retrata o artigo 25.º, que tem um vasto conjunto de obrigações.

O RGPD, desdobra e desenvolve a obrigação da implementação de medidas técnicas e organizativas em duas vertentes: a da segurança dos dados (artigo 32.º) e as exigências em função dos direitos e obrigações gerais contemplados no respetivo regulamento (arts.º24 e 25) (Pinheiro et al. 2018).

O considerando 78 do RGPD, diz respeito à defesa dos direitos e liberdades relativamente ao tratamento de dados pessoais direcionadas a pessoas singulares, as organizações devem implementar medidas técnicas e organizativas de forma a demonstrarem que consideram e integraram medidas de conformidade com as regras de proteção de dados nos tratamentos de dados, do presente regulamento (cf. artigo 25.º, n.º 1 e 2, do RGPD).

Este artigo exige a criação de salvaguardas para satisfazer os requisitos de todo o GDPR e proteger os direitos do titular dos dados. Isso exige que as entidades responsáveis das empresas criem salvaguardas técnicas ou organizacionais apropriadas aos sistemas, levando em consideração o estado da arte, o custo de implementação e a natureza, escopo e finalidade do processamento (Urquhart, Sailaja, and McAuley 2019).

Levando em conta as considerações mencionadas, bem como os riscos para os direitos e liberdades das pessoas singulares representadas pelo processamento, o responsável pelo tratamento deve, tanto no momento da determinação dos meios de processamento quanto no momento do próprio processamento, implementar procedimentos técnicos adequados e medidas organizacionais, como a pseudonimização, projetadas para implementar princípios de proteção de dados, como minimização de dados, de maneira eficaz e para integrar as salvaguardas necessárias ao processamento, a fim de atender aos requisitos deste regulamento e proteger os direitos dos titulares dos dados (cf. artigo 25.º, n.º 2, do RGPD).

Em concordância, Batalha (2017), defende que a referência do RGPD, alude ao tratamento de dados, considerando que este realiza operações sobre dados pessoais ou sob um conjunto dos mesmos. Tratamento esse disponibilizado através da recolha, do registo, da gestão, recuperação, consulta, formas de divulgação da informação, interconexão, limitação e o apagamento/destruição.

Paralelamente, os dados mesmo sendo cifrados ou pseudonimizados podem continuar a serem considerados como dados pessoais, pelo que concerne a cada organização a identificação dos processos que envolvem dados pessoais suscetíveis a serem acedidos. É ainda de responsabilidade dos próprios, avaliar os riscos e definir métodos/técnicas que garantam o tratamento apropriado, considerando como hipóteses a anonimização ou eliminação, caso deixem de ser úteis para a finalidade inicial ou não houver uma boa gestão dos mesmos (Pinho, Correia, and Antunes 2017).

O regulamento introduz o conceito de pseudonimização, como o "tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;" (cf. artigo 4.º, n.º 5, do RGPD)

Segundo Finck e Pallas (2019), apud Miranda Mourby (2018) afirma que a pseudonimização não é um método de anonimização, mas que reduz a capacidade de vinculação de um conjunto de dados com a identidade original de um titular de dados e, portanto, refere ser uma medida de segurança útil. Vale ressaltar que, o RGPD evidencia claramente a pseudonimização como uma abordagem valiosa de minimização, além de uma medida de gestão de riscos.

Em vista disso, um risco é considerado um conceito central da lei europeia da proteção de dados. Embora a sua definição seja usada em diferentes contextos, as repetidas referências sublinham que as obrigações referidas no regulamento são, sob muitos aspetos, formas para lidar com o risco aos direitos e liberdades dos titulares de dados que surgem quando os dados pessoais estão a ser processados (cf. considerando 26, do RGPD).

A pseudonimização pode servir como ponto de conformidade com a obrigação da segurança do controlador (cf. artigo 5.º, (f), do RGPD) e confirmar que a proteção de dados desde a conceção e por defeito foi devidamente considerada (cf. artigo 25.º, do RGPD).

Quando ocorre uma violação de dados, o responsável pelo tratamento está livre de acionar as obrigações de notificação, onde possa demonstrar que a violação resulte num risco para os direitos e liberdades das pessoas, portanto, os códigos de conduta devem equilibrar as obrigações dos controladores com base no risco resultante do tratamento. Seria uma boa ação, a implementação (por parte do controlador) de medidas técnicas e organizacionais que considerem vantajosas, bem como o risco que acarreta o direito e liberdade das pessoas (Finck and Pallas 2019).

Do mesmo modo que nos termos do artigo 25.º, a proteção de dados desde a conceção e por defeito devem ser equilibrados com base nos riscos. Nesse sentido, as Avaliações de Impacto na Proteção de Dados (*DPIAs*) são necessárias quando o tratamento resulta num "alto risco para os direitos e liberdades das pessoas físicas". Ao mesmo tempo, sabe-se que o anonimato é importante na Proteção de Dados desde a Conceção (*DPbD*), no entanto, de acordo com Raphael Gellert (2019), nunca poderá haver uma forma absoluta de anonimização, havendo sempre presente um risco residual de identificação. Documentos de orientação geral, como diretrizes ISO sobre a gestão de risco tornam-se úteis nestes assuntos (Finck and Pallas 2019).

3.4.1. Princípio da proteção de dados desde a conceção

Tal como se observa, o RGPD, demonstra ser extremamente vago sobre o que a *DPbD* significa, não reconhecendo, não referido nos considerandos nem nos artigos do mesmo a promulgação,

ou as situações onde eventualmente poderá haver conflito de escolha nas abordagens da Privacidade desde a conceção (*PbD*).

A *PbD*, e o *DPbD* agora exigido por lei, é visto cada vez mais como sinônimo sobre tecnologias para aumentar a privacidade, que toma como objetivo único reduzir a divulgação de informações indesejadas. Essas literaturas, sem dúvida, fornecem ferramentas úteis tanto para os titulares de dados quanto para os controladores.

See Reuben Binns (2019), refere que as *DPIAs* são posicionadas como sendo um ponto adequado no processo da conformidade para a implantação de estratégias de *DPbD*. Os *DPIAs* são a principal análise preventiva e de requisitos de documentação no RGPD, tendo como objetivo particular o processamento de alto risco, mas são intransparentes com a falta de requisitos de publicação (Veale, Binns, and Ausloos 2018).

Segundo Veale, Binns e Ausloos (2018), apud Ann Cavoukian (2017) refere que a *PbD* não é simplesmente um conjunto de medidas organizacionais e técnicas para impedir a divulgação de informações, mas com o intuito de mapear da maneira mais ampla a ideia de privacidade, que deixa o objetivo claro de garantir a privacidade consagrada nos direitos e princípios da proteção de dados, em vez da privacidade geral.

Numa outra perspetiva, Lee Bygrave afirma que os requisitos da Proteção de Dados desde a Conceção (*DPbD*), impõem um dever qualificado aos controladores de implementar medidas técnicas e organizacionais destinadas a implementar efetivamente os princípios de proteção de dados e integrar salvaguardas necessárias ao tratamento de dados pessoais, para que esse tratamento cumpram os requisitos do regulamento e garantam a proteção dos direitos dos titulares de dados (cf. artigo 25.º, do RGPD).

Um controlador de dados, fornece informações necessárias para garantir um processamento justo e transparente, incluindo a "existência do direito de solicitar ao controlador acesso e retificação ou apagamento de dados pessoais." (cf. artigo 13.º e 14.º, do RGPD)

As organizações devem "implementar medidas técnicas e organizativas de forma a demonstrar que consideraram e integraram medidas de conformidade com as regras da proteção no tratamento dos dados. Devem incidir sobre dados que sejam realmente necessários para o prosseguimento das finalidades específicas do tratamento" (Fazendeiro 2018).

À proporção das medidas a serem tomadas entre elas estão as técnicas potenciadoras da proteção dos titulares de dados, que introduzida no RGPD, se destaca o conceito de

pseudonimização. Conceito este definido como "ato de anonimizar o tratamento de dados, de tal forma que, não possa ser atribuído a um indivíduo específico, sem a utilização de informação adicional" (Mamede 2015). As informações suplementares devem ser mantidas separadas e sujeitas a medidas técnicas organizativas para assegurar que os dados pessoais não possam ser atribuídos a pessoas identificáveis (cf. artigo 4.º, n.º 5, do RGPD).

Contudo, é imprescindível a utilização de aplicações, serviços e produtos no tratamento de dados pessoais para a execução das suas funções, tal como garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações referentes à proteção de dados.

Além disso, as empresas devem garantir que o uso dos dados pessoais está de acordo com as normas implementadas no RGPD desde o momento da sua recolha, das fases de tratamento, até à sua destruição. Adicionalmente, deve ser assegurado que os dados devem ser utilizados meramente para as finalidades para os quais foram recolhidos. Sem embargo, os autores Hildebrandt e Tielemans (2013), partilham da opinião de que, um dos aspetos mais desafiadores proposto no RGPD, é a obrigação de os responsáveis dos dados garantirem s *DPbD*. Ao que tudo indica, parece iniciar um novo tipo de conceito jurídico, pelo qual o regulamento se alinha ao conceito de ética e política, orientado para a política de privacidade, onde garante a segurança desde a sua implementação.

Atualmente diversas entidades informáticas, utilizam a compactação dos dados referenciados em áudios, de modo a processar a sua transição para os servidores das empresas e retornando aos dispositivos iniciais. Estes sistemas utilizam uma abordagem sem precedentes no reconhecimento da voz, sem uso intensivo de energia ou armazenamento no dispositivo tecnológico. Um dos principais objetivos deste sistema é fornecer um assistente de voz personalizado para um individuo (cf. artigo 11.º, do RGPD).

Normalmente, usa-se essa tecnologia para ativar funcionalidades nas quais estão associadas com o serviço, controlar e criar documentos ou mensagens. Como exemplo, a "Google", fornece uma ferramenta na qual os dados de voz e áudio podem ser pesquisados e geridos, por outro lado, a Apple além de fornecer o serviço da assistente de voz idêntico aos adversários, não fornece dados automáticos aos titulares dos dados, nem as solicitações presentes na sua Lei da Proteção de Dados de origem.

De acordo com Veale, Binns, e Ausloos (2018), alegam a *PbD* como motivo do não fornecimento de dados automáticos aos titulares dos dados, razões como como identificadores

específicos de dispositivos separados das identidades dos utilizadores (*Apple* alegou que não possuía um meio técnico para aceder ao identificador do serviço de voz no dispositivo, nem para pesquisar dados por identificador, pois optaram por não criar um). Identificadores vinculados são tratados e excluídos após intervalos de meses para que o sistema possa entender a voz do utilizador e guardar no período de dois anos para melhorar o desenvolvimento do serviço do assistente de voz, além de gravações de músicas e pontos de interesse dos utilizadores.

Apesar da falta de requisitos detalhados relacionados com o direito da informação, espera-se que os controladores de dados possam demonstrar conformidade com as disposições do RGPD (obrigações de segurança e *DPbD*). Desse modo, devido às faltas das publicações dessas informações, muitas das soluções para o ambiente de tratamento são cada vez mais complexas e correm o risco de obter informações complexas sobre a recaída dos sistemas computacionais. Em vez disso, colocar terceiros como beneficiários de alguns direitos da informação seria um passo futuro útil.

Embora as Autoridades de Proteção de Dados (*DPAs)* tenham aumentado significativamente o domínio de investigar controladores de dados, isso geralmente acontece apenas depois que uma reclamação é erguida (Veale, Binns, and Ausloos 2018).

É difícil fazer uma reclamação sobre aplicativos impróprios ou ineficazes de privacidade ou *DPbD*, sem algumas informações sobre a infraestrutura do sistema (até que esses sistemas falhem de maneira ampla e percetível). O tratamento de alto risco (riscos que não podem ser suficientemente atenuados) devem envolver uma consulta e autorização prévia do *DPA* responsável.

3.4.2. Implementação de medidas técnicas e organizacionais

Muitas das violações de informações informáticas de mais alto nível, representam dados identificáveis, como nomes completos, endereços de residência/digitais, ID's ou números de telefone, e entrar em contacto com o individuo afetado é uma incumbência, que permite um canal de comunicação entre o *DPO* e o individuo. Atualmente, cada vez mais é a dimensão de casos de rastreamento via *web*, através de históricos de navegação nos *browsers* ou *plugins*, que se tornaram modalidades vulneráveis.

Ferramentas como *cookies*, impressões digitais de *browsers* ou identificadores específicos de dispositivos não são considerados meios identificáveis para ser transmitido um canal de comunicação até ao individuo. No entanto, esses recursos regularmente recolhidos por "redes de publicidade comportamental", agem desse modo, precisamente para de alguma forma se comunicarem com os utilizadores através do meio específico de anúncios dos *browsers* (Veale, Binns, and Ausloos 2018).

A necessidade de as empresas adotarem medidas e procedimentos técnicos, que tornem os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acede-los, ou medidas subsequentes para mitigar riscos, visam garantir se o tratamento dos dados está em conformidade com o RGPD, assim como a proteção dos direitos dos titulares de dados associados. Desta forma, com os riscos decorrentes do tratamento, contexto e finalidades, o responsável pelo tratamento deve implementar, no momento da definição dos meios de tratamento, as medidas procedimentais e organizativas adequadas com êxito, os princípios estipulados no RGPD (Magalhães and Pereira 2018).

No que concerne à adoção das medidas técnicas ou organizacionais, as mesmas podem variar, realizando utilizações de soluções técnicas avançadas ou básicas (saber lidar com os dados dos clientes). A implementação dos princípios da proteção de dados significa que a entidade reguladora incorporou as medidas necessárias para garantir a sua eficácia ao longo do ciclo de vida dos dados pessoais que estão a ser processados.

Segundo o Conselho Europeu para a Proteção de Dados (2019), permitir que os titulares de dados intervenham no tratamento, de modo a fornecer informações automáticas e repetidas sobre quais dados pessoais estão armazenados, ou ter um lembrete de retenção num repositório de dados, são consideradas medidas de proteção. Adicionalmente, também é considerada medida, a implementação de um sistema de deteção de *malware*[13] numa rede de computadores, o que seria útil para uma pós-formação de funcionários sobre conceitos informáticos, como *phishing*[14].

No entanto, a principal medida técnica adotada nas organizações é a pseudonimização dos dados pessoais. A medida pode ser utilizada na implementação de uma série de princípios, como a integridade, confidencialidade e minimização de dados (cf. artigo 4.º, n.º 5, do RGPD).

13 Parte de um software que tenha sido codificada com o objetivo de danificar dispositivos, roubar dados e causar danos às pessoas, como vírus, cavalos de tróia, *spywares* e *ransomwares*. Disponível em: (https://www.avg.com/pt/signal/what-is-malware) (Consultado em 24-12-2019)

14 Forma desonesta dos cibercriminosos usarem indivíduos para revelar informação pessoal, como senhas, cartões de crédito ou contas bancárias. Disponível em: (https://www.avast.com/pt-br/c-phishing) (Consultado em 28-12-2019)

No entanto, a *PbD* vai além das manobras de segurança. Schaar (2010), sustenta a ideia de que os sistemas devem ser projetados e construídos de maneira a evitar ou minimizar a quantidade de dados pessoais processados.

Se como referido, o *DPbD* corre o risco de retirar direitos, como podemos corrigir ou melhorar estas situações? Veale, Binns e Ausloos (2018) propõem abordagens que podem ajudar, avaliar as possibilidades e colocá-las no contexto jurídico. Primeiramente, sistemas projetados para a retenção de dados (com o objetivo de fornecer acesso e permitir melhor cumprimento de oposição e apagamento) e sistemas projetados para processar dados adicionais (podem ser fornecidos pelo titular dos dados para possível reidentificação)

Consequentemente, quando esses mecanismos de reidentificação são publicados nas páginas de literatura dos *browsers* (onde a base dos códigos é imprecisa/não confiável), são precisamente esses os tipos de ferramentas com as quais atacantes *"script-kiddie*[15]*"* estão frequentemente acostumados a trabalhar. Imaginar que, tornar essas ferramentas mais úteis e implantáveis servirá apenas para ajudar os invasores, além de subestimar a capacidade existente dos adversários de gerirem conhecimento para valorizar dados pessoais roubados.

Insistimos para que a sociedade apoie no desenvolvimento das tecnologias de reidentificação, a fim de permitir aos titulares de dados serem localizados em conjuntos de dados não identificáveis, para que se possa gerir melhor os riscos. As ferramentas de reidentificação são constantemente desenvolvidas, no entanto, as bases de código para essas ferramentas são muito instáveis e de custo elevado para facilitar o uso aos controladores dos titulares de dados.

3.4.3. Princípio da proteção de dados por defeito

Segundo o Conselho Europeu para a Proteção de Dados (2019), o conceito "*Default*", em segurança da informação, refere-se a um valor pré-existente adotado por um programa de computador ou outro mecanismo quando nenhuma alternativa é especificada pelo utilizador ou programador. Normalmente, essas configurações em contexto informático são chamadas de "predefinições de fábrica", especialmente para dispositivos eletrónicos.

O responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir que apenas sejam processados os dados pessoais necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados

[15] Atacantes/hackers aprendizes ou a iniciantes.

pessoais recolhidos, à extensão do seu tratamento, ao prazo de armazenamento e à sua acessibilidade. Em particular, essas medidas devem garantir que, por defeito, os dados pessoais não sejam acessíveis sem a intervenção do indivíduo a um número indefinido de pessoas físicas (Faria, Pinto, and Antunes 2018).

As entidades reguladoras, devem garantir que, deverão ser ativados apenas os dados pessoais necessários para atingir o objetivo do tratamento. Neste caso, os responsáveis pelo tratamento de dados, devem basear-se na avaliação da necessidade do tratamento no que respeita aos fundamentos legais do artigo 6.º, n. º1 ("Licitude do Tratamento"). Este artigo refere que caso o responsável use um *software* de terceiros, e as funções que não possuam cobertura por motivos legais ou que não sejam compatíveis com os objetivos pretendidos, estas sejam desativadas (cf. artigo 6.º, n.º 1, do RGPD).

As mesmas considerações aplicam-se às medidas organizacionais que dão suporte às operações de tratamento. Os mesmos devem ser intencionados para processar, desde o início, apenas a quantidade mínima de dados pessoais necessários para as operações específicas. Isso deve ser particularmente considerado ao determinar o acesso aos dados para equipas com funções organizacionais diferentes (Conselho Europeu para a Proteção de Dados 2019).

Numa era em que a recolha de dados é facilmente despercebida em grande escala, o legislador europeu recorda o dever dos responsáveis pelo tratamento, de determinar a recolha e o tratamento ao mínimo necessário e proporcional às finalidades do tratamento. (Pinheiro et al. 2018).

4. Contexto normativo

4.1. Série de normas de segurança da informação

Um ambiente que lida com SI, é considerado complexo, de acordo com as conexões de redes remotas, sistemas de armazenamento e servidores. Garantir a segurança é considerada uma tarefa extensa e complicada que, sem a devida atenção poderá causar danos e surgir consequências.

Dado isso, e de acordo com Stallings (2015), as normas que auxiliam a garantir a segurança da informação nas organizações têm-se tornado cada vez mais fulcrais em tais circunstâncias. O autor refere ainda que, as normas auxiliam a definir a finalidade das funções e dos recursos de segurança necessários, das políticas de gestão da informação e recursos humanos, dos critérios para avaliar a eficácia dos parâmetros de segurança, técnicas para avaliação contínua da segurança e o controlo das violações de segurança e procedimentos para lidar com as respetivas falhas.

Em conformidade, Dey (2007), refere que as normas de segurança fornecem uma abordagem da gestão para a implementação e melhoria das práticas de segurança, através do estabelecimento de um Sistema de Gestão de Segurança da Informação (SGSI), na qual permite identificar na organização os pontos vulneráveis e as falhas nos sistemas que deverão posteriormente ser corrigidos. Princípio desenvolvido com o intuito de se vir a tornar a norma global de SI: o conjunto ISO/IEC 27000. Em concordância com o autor, T. R. Oliveira (2017), alude que as normas se destinam a recomendar requisitos e controlos que consistam em garantir uma factual segurança da informação.

No mesmo contexto, Disterer (2013) aponta que esta norma visa fornecer o controlo de objetivos e específicos, requisitos e diretrizes, com os quais as organizações poderão obter uma segurança da informação apropriada. O autor ainda refere que se uma organização procurar estar em conformidade com estas normas, promove não só a confiança entre clientes, mas também a redução do risco das multas ou pagamentos de compensação como resultado de litígios legais, uma vez que através da conformidade de padrões das normas, estes problemas poderão ser combatidos.

Após uma profunda análise das normas de segurança, destacam-se as normas ISO/IEC 27000 e 27001, que consistem em "perceber os pressupostos relacionados com a Segurança da Informação. Esta temática atualmente tem bastante importância, uma vez que se fala muito

em ataques de *hackers* contra plataformas digitais, que tentam aceder a informação confidencial. A informação é um bem com bastante valor para as organizações e necessita de ser convenientemente protegida, no sentido de manter a sua confidencialidade, disponibilidade, integridade e autenticidade" (Cruz 2012).

Nesta perspetiva, as normas 27001 e 27002 estão bastante relacionadas com a segurança de dados digitais ou sistemas de armazenamento eletrónico. A definição segurança da informação vai além da questão informática e tecnológica, apesar de serem contíguos. Contudo, é importante realçar que a série de normas 27000 abrange um total de 45 normas, das quais 39 já foram publicadas e 6 estão em desenvolvimento (International Organization for Standardization 2020). No entanto, cada uma destas normas tem foco em um aspeto de segurança específico. São reveladas as potenciais normas na tabela 2, que se correlacionam com domínios específicos da segurança da informação:

Norma	Ano	Área de Domínio (Information Technology/Security Techniques)	Certificação
ISO/IEC 27001	2013	Information security management systems - Requirements	2019-06-03
ISO/IEC 27002	2013	Code of practice for information security controls	2018-03-26
ISO/IEC 27003	2017	Information security management systems — Guidance	2017-04-12
ISO/IEC 27004	2016	Information security management - Monitoring, measurement, analysis and evaluation	2016-12-15
ISO/IEC 27005	2018	Information security risk management	2018-07-09
ISO/IEC 27006	2015	Requirements for bodies providing audit and certification of information security management systems	2015-09-30

Tabela 2 - Principais Normas da Segurança da Informação

Fonte: elaboração própria

4.1.1. A ISO 27001: gestão de segurança da informação

Devido à alta quantidade de informação e o baixo nível de segurança nos processos de modificação do mercado, os mesmos colocam-se em risco em relação à produtividade da organização. A ISO/IEC 27001 é a norma internacional mais adotada pela norma de gestão de segurança da informação (Shojaie, Federrath, and Saberi 2015). Considerada uma norma de gestão e avaliação de processos, fornece especificações para um Sistema de Gestão de Segurança da Informação (SGSI) (Shivashankarappa et al. 2012).

Na abrangência do conteúdo e atendendo às suas características, segundo Shojaie, Federrath e Saberi (2014), a norma consiste em duas partes: a primeira parte fornece os requisitos para que um SGSI seja implementado, mantido e aprimorado, enquanto a segunda parte é o Anexo A, que define os objetivos de controlo e os controlos de segurança. Esse anexo, enumera um vasto conjunto de controlos e outras medidas relevantes para a segurança da informação.

Particularmente, a ISO 27001: 2013 é uma versão retificada da ISO 27001: 2005. Na norma do ano de 2005, o anexo A contém 133 controlos com 11 categorias, enquanto a versão atualizada contém apenas 114 controlos em 14 categorias (Nasser 2017). Na tabela 3 apresenta-se as alterações nos domínios do respetivo anexo (Maingak, Candiwan, and Harsono 2018).

	ISO/IEC 27001:2005	Revisão da ISO/IEC 27001:2013
A.5	*Security policy*	*Information security policies*
A.6	*Organisation of Information Security*	*Organization of information security*
A.7	*Asset management*	*Human resources security*
A.8	*Human resources security*	*Asset management*
A.9	*Physical and Environmental Security*	*Access control*
A.10	*Communications and Operation Management*	*Cryptography*
A.11	*Access control*	*Physical and environmental security*
A.12	*IS Acquisition, Development and Management*	*Operational security*
A.13	*Information security incident management*	*Communication security*

A.14	*Business continuity management*	*System acquisition, development and maintenance*
A.15	*Compliance*	*Supplier relationship*
A.16	-	*Information security incident management*
A.17	-	*Information security aspects of business continuity management*
A.18	-	*Compliance*

Tabela 3 - Modificações na ISO/IEC 27001 (Anexo A)

Fonte: elaboração própria

Os objetivos de controlo e os controlos de segurança referidos no Anexo A, não são de todo exaustivos, além de poderem ser necessários objetivos de controlo complementares, sendo estes do A.5 a A.18. No entanto, estas diretrizes são derivadas diretamente com a ISO/IEC 27002:13 nas mesmas secções da norma.

É fulcral mencionar que os objetivos de controlo e os controlos de segurança estão definidos em oito secções, todavia, a ordem dos mesmos não tem a essência de referir o seu nível de importância.

Secção	Descrição dos objetivos de controlo	Nº. Categorias	Nº. Controlos
A.5	Políticas de segurança da informação	1	2
A.6	Organização de segurança da informação	2	7
A.7	Segurança na gestão de recursos humanos	3	6
A.8	Gestão de ativos	3	10
A.9	Controlo de Acessos	4	14
A.10	Criptografia	1	2
A.11	Segurança física e ambiental	2	15
A.12	Segurança de operações	7	14

A.13	Segurança de comunicações	2	7
A.14	Aquisição, desenvolvimento e manutenção de sistemas		13
A.15	Relações com fornecedores	2	5
A.16	Gestão de incidentes de segurança da informação	1	7
A.17	Aspetos de segurança da informação na gestão da continuidade do negócio	2	4
A.18	Conformidade	2	8

Tabela 4 - Objetivos de controlo e os controlos de segurança

Fonte: elaboração própria

Como refere a tabela 4, cada secção é composta por um número exato de categorias principais relativas à segurança da informação. Assim como cada categoria contém um controlo que define o modo de como o objetivo deve ser alcançado e um ou mais controlos (subcontrolos) que eventualmente poderão ser aplicados para alcançar o mesmo objetivo definido.

A *International Organization for Standardization*, realiza diversas certificações para a gestão de normas, anualmente. A investigação evidencia o número de certificados emitidos por organismos que foram certificados por membros do IAF [16]. Com base no caso de estudo de 2017, conclui-se que há um aumento de 7,9% na certificação ISO/IEC 27001 mundialmente (Charlet 2017). Paralelamente, de acordo com o mais recente caso do ano de 2018, o número total geral de certificados válidos foi menor que em 2017.

Apesar da notória regressão, a International Organization for Standardization (2019), exibe o número total de certificados válidos e o número total de sites para cada modelo de norma[17]. Portanto, a norma 27001:2013 indigita os seguintes valores:

a. Total de certificados válidos: 31 910

[16] Associação mundial de organismos de acreditação para avaliação de conformidade. Programa mundial de avaliação da conformidade, que reduz o risco para as empresas e os seus clientes, de forma a garantir aos mesmos que os certificados acreditados podem ser confiáveis. Disponível em: (https://www.iaf.nu/) (Consultado em 23-11-2019)

[17] Os resultados detalhados para cada norma estão disponíveis no site da ISO. Disponível em: (https://www.iso.org/the-iso-survey.html) (Consultado em 22-12-2019)

b. Número total de sites: 59 934

Convém salientar que um certificado é um "documento emitido por um organismo de certificação, uma vez que o cliente demonstrou conformidade com a norma", assim como um site é um "local permanente em que uma organização realiza trabalho ou serviço" (International Organization for Standardization 2019).

Segundo a International Organization for Standardization (2019), os motivos da diminuição estão relacionados com a sua participação:

- Organismos de certificação relataram em investigações anteriores o número de certificados que incluíam o número de sites. Nesta investigação, eles dividiram o número de certificados e o número de sites, o que levou a uma importante redução no número de certificados relatados;
- Dados relatados por organismos de certificação variam de um ano para outro;
- Organismos de certificação importantes em alguns países não participaram.

Ainda no âmbito deste projeto, conclui-se que a "ISO/IEC 27001 faz parte de um sistema de gestão de uma organização baseada em uma abordagem de risco comercial que visa criar, implementar, operar, observar, manter e melhorar a segurança da informação.", ou seja, esta norma permite à organização ou à empresa comparar a concorrência e fornecer informações relevantes sobre segurança das TI (Peciña, Bilbao, and Bilbao 2011).

4.1.1.1. Implementação da metodologia cíclica PDCA

No que acontece com outros padrões das TI, a série de normas SGSI, refere-se diretamente a uma metodologia cíclica, designada de *Plan - Do - Check – Act/Adjust* (PDCA), conhecido pela na área da gestão da qualidade por *Deming*[18] (Disterer 2013), no entanto considera-se recomendada para garantir a melhoria continua do Sistema de Gestão de Segurança da Informação (SGSI) (Funk et al. 2016).

O autor Cruz (2012), refere que um processo é a "transformação de entradas em saídas que utilizam um conjunto de atividades interrelacionadas ou em interação. A saída de um processo

[18] *Dr. W. Edwards Deming* tornou-se popular no controlo da qualidade moderna, criador do ciclo metodológico *PDCA*. Disponível em: (https://pt.wikipedia.org/wiki/William_Edwards_Deming) (Consultado em 13-12-2019)

pode involuntariamente dar início a um novo processo, isto é feito normalmente de forma planeada", necessariamente sob condições controladas.

Nessa abordagem, e segundo Disterer (2013), o ciclo permite enfatizar a necessidade da orientação dos processos, bem como a integração do planeamento das ações e a verificação continua da implementação em conformidade com o seu planeamento:

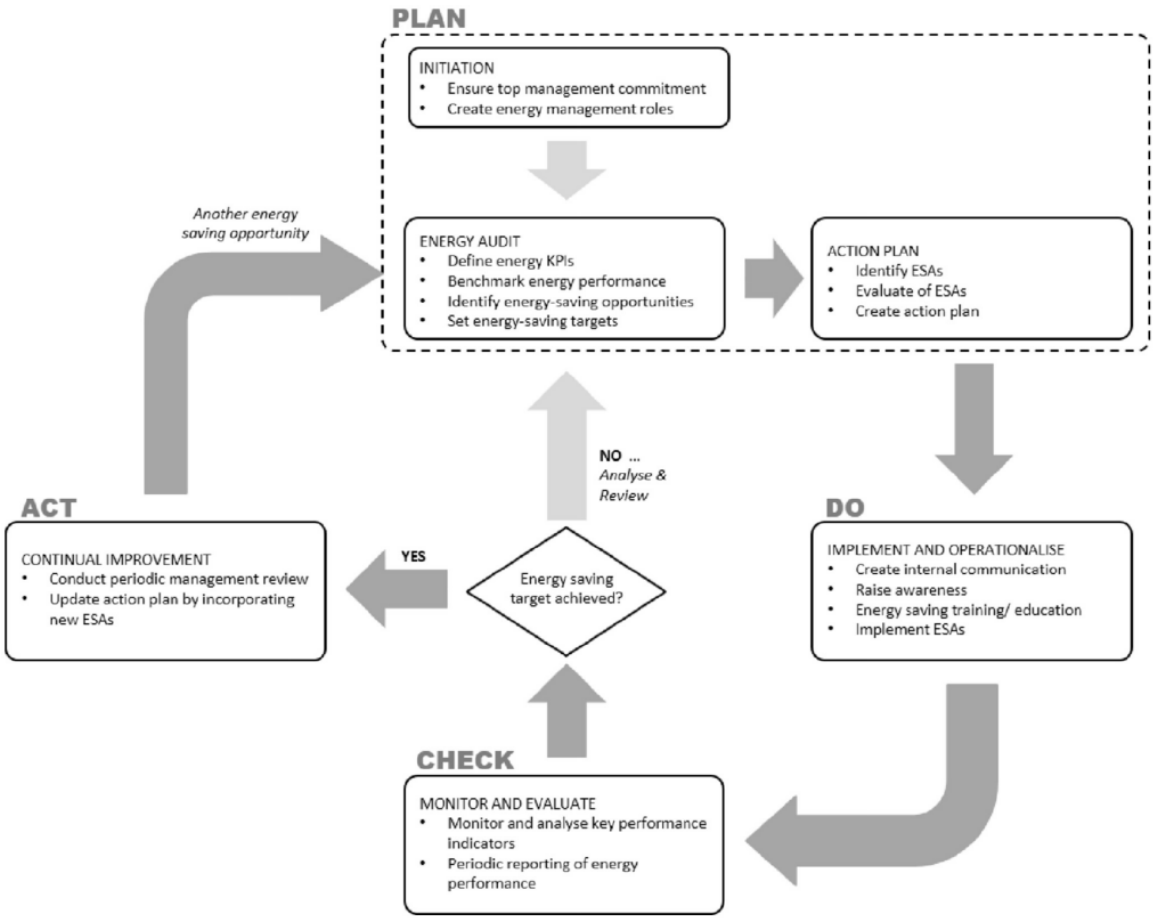


Figura 3 - Ciclo PDCA aplicado aos processos de um SGSI

Fonte: Prashar (2017)

Na perspetiva de uma melhor abrangência ás etapas representadas, o autor Velasco et al. (2018) generaliza de forma sucinta os conceitos aludidos da figura 3:

- ✓ Na primeira etapa, "*Plan*", pretende-se estabelecer a política, objetivos, processos e procedimentos do SGSI relevantes para a gestão de riscos e melhoria da segurança da informação.
- ✓ Na segunda etapa, "*Do*", estabelece-se os requisitos para medir o funcionamento do

SGSI, as expectativas da alta gerência e o seu *feedback*. Necessário para atender aos objetivos e requisitos de segurança e para realizar a avaliação e tratamento de riscos de informação de segurança.

- ✓ Posteriormente, temos a etapa "*Check*", que define os requisitos para medir e avaliar o desempenho do SGSI, periodicamente.
- ✓ Por fim, a etapa "*Act*", estabelece o processo de melhoria do SGSI, com base nas "não conformidades" identificadas na organização. Nesta fase, as ações devem ser estabelecidas para as resolver ou descartar (Gonzales 2018).

É necessário a execução de alguns procedimentos de acordo com o ciclo PDCA, dado isso, de acordo com os quatro objetivos do ciclo a cumprir menciona-se os principais métodos a aplicar (Funk et al. 2016; Gonzales 2018) :

1. *"Plan"* (Planificar)

a. Definir o plano de tratamento: ações, recursos, responsabilidades e prioridades;
b. Estabelecer objetivos dos controlos e os responsáveis pelos processos operacionais;
c. Estabelecer medidas de segurança para atingir os objetivos de controlo (definir políticas de segurança);
d. Criar procedimentos e métricas para avaliação do Risco;
e. Avaliação dos riscos de segurança da informação;

2. *"Do"* (Implementar e Executar)

a. Avaliação contínua do alcance dos objetivos (entregues ao controlo de segurança);
b. Tratamento de Risco;
c. Implementar controlos (controlos já estabelecidos para cada processo são aplicados);
d. Verificar segurança de informação organizacional;
e. Verificar manual da política de segurança da informação;
f. Sensibilização e consciência (funcionários devem estar motivados sobre a importância da aplicação do SGSI);
g. Gerir operações e recursos do SGSI;
h. Implementação de ações corretivas se forem identificadas falhas ou não-conformidades (Desenvolver as normas e procedimentos de segurança da informação).

3. *"Check"* (Auditoria e Teste)

a. Procedimentos de monitorização e de controlos devem ser aplicados para expor erros e identificar violações e incidentes de segurança;

b. Medir a eficácia dos controlos: implementar métodos de monitorização para medir a eficácia dos controlos que estabelecem indicadores e métricas de gestão;
c. Retificar regularmente a avaliação dos riscos (influenciar mudanças na organização, tecnologia, processos e objetivos de negócios, ameaças, eficácia dos controlos);
d. Realizar análises internas regularmente (conformidade com os requisitos estabelecidos pela ISO/IEC 27001);
e. Elaboração de relatórios de segurança (incluem recomendações de ação para as decisões administrativas, ou caso possa impactar o desempenho ou o SGSI).

4. *Act"* (Manter e melhorar)

a. Implementar melhorias (todas as melhorias propostas nas fases anteriores devem ser implementadas);
b. Ações corretivas, para resolver "não conformidades" detetadas;
c. As decisões tomadas são documentadas adequadamente (através do controlo de segurança), incluindo explicações, nas quais devem ser divulgadas a todos os funcionários de acordo com o nível da hierarquia.

Ao aplicar esta metodologia de *Deming*, o ciclo PDCA, como ferramenta de desenvolvimento contínuo, pretende-se alinhar os processos instáveis da área de operações. O PDCA garante a "confidencialidade, integridade e disponibilidade de informação, para a gestão correta nos níveis lógicos e físicos, com benefícios a curto prazo" (Velasco et al. 2018).

A implementação de um SGSI tem como principal resultado a redução dos riscos de segurança da informação, ou seja, reduzir a probabilidade de ocorrerem incidentes a nível de segurança da informação e consequentemente reduzir os seus impactos. Este sistema para ser passível de ser certificado tem de obedecer a um conjunto de requisitos definidos pela norma ISO/IEC 27001 (Cruz 2012).

4.1.1.2. Abordagens benéficas aplicáveis a nível organizacional

A alegada norma universal, que colabora com todo o tipo de organizações, transmite flexibilidade na determinação dos requisitos para a prática de implementação de controlos de segurança que podem ser modificados conforme a imposição da organização.

Como todos os outros padrões de normas, é possível a certificação da ISO/IEC 27001, porém não obrigatória. No entanto, Stallings (2015), reforça a ideia de que cada vez mais as entidades

responsáveis pelos SI reconhecem a importância da adoção das boas práticas e normas universais, na qual, consideram ser uma crescente utilização para o sucesso dos projetos empresariais.

Independentemente das entidades organizacionais deliberarem ou não a certificação, a adoção de práticas de gestão documentadas na considerada norma, representa um conjunto de regalias e vantagens, notadamente (Correia and Santos 2016) :

1. Demonstrar um compromisso dos Executivos da Organização para com a segurança da informação (problema atual devido à confiança do tratamento apropriado da informação sensível na organização);
2. Aumentar a idoneidade e a segurança dos SI, em termos de confidencialidade, disponibilidade e integridade;
3. Garantir a realização de investimentos mais eficientes e orientados ao risco, ao invés de investimentos baseados em tendências;
4. Modernizar os níveis de sensibilidade, participação e motivação dos funcionários para com a segurança da informação.
5. Identificar e expedir processos e oportunidades de melhorias, de forma contínua;
6. Aumentar a confiança e satisfação dos clientes e integrantes, proporcionando um maior potencial para realização de posteriores negócios;
7. Implementação dos controlos provenientes da norma e da análise de risco, capaz de melhorar o desempenho operacional das organizações;
8. Beneficiar a organização com um SGSI, incrementando a eficácia da organização;
9. Conceder a organização com ferramentas que demonstrem o cumprimento do regulamento UE 2016/679 no tratamento e circulação de dados pessoais.

De acordo com Correia e Santos (2016), apud Silva (2011), este refere que “a obtenção de certificações através de normas de Gestão da Segurança de Sistemas de Informação é tida como promotora e evidenciada dos esforços de proteção do sistema de informação por parte das organizações.” O autor aludido menciona ainda que, a identificação de benefícios da obtenção da certificação pode auxiliar os responsáveis organizacionais a constatar a qualidade das condições para se estender para um processo de certificação bem-sucedido, de modo a que estas estejam perpetuamente a gerir o nível de fatores inibidores para a obtenção do mesmo.

4.1.2. A ISO 27005: gestão de riscos à segurança da informação

Um dos tópicos sugeridos na norma ISO/IEC 27001 faz referência às organizações que carecem o dever de realizar avaliações de risco da segurança da informação, recomendam a implementação de um plano de tratamento de risco e estas devem manter a informação documentada dos resultados do tratamento do risco de segurança da informação. A diretiva está associada com a crescente dependência das empresas dos SI/TI (R. A. P. Oliveira and Respício 2015).

A norma NP ISO/IEC 31000:2018 define risco de uma forma geral: "Efeito da incerteza na consecução dos objetivos. Um efeito é um desvio, positivo ou negativo, relativamente ao esperado. Os objetivos podem ter diferentes aspetos (financeiros, saúde, segurança, ambientais) e podem ser aplicados a diferentes níveis (estratégico, em toda a organização, de projeto, de produto e de processo). O risco é frequentemente caracterizado pela referência aos eventos potenciais e consequências, ou à combinação de ambos. A incerteza é o estado, ainda que parcial, de deficiência de informação relacionado com a compreensão ou conhecimento de um evento, sua consequência ou probabilidade" (NP ISO/IEC 31000 2018).

Como referenciado anteriormente, a ISO/IEC 27005 contém diretrizes associadas à implementação de um SGSI com base na abordagem da gestão do risco. Contudo, esta norma contém a estrutura aplicacional da norma NP ISO/IEC 31000 "Gestão do Risco – Diretrizes", que tem como objetivo fornecer princípios e linhas de orientação gerais sobre a gestão do risco, podendo ser aplicada em qualquer tipo de organização, de modo a poderem integrar estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos (Correia and Santos 2016).

Complementarmente, a ISO/IEC 27005 pretende servir de base a algumas definições mencionadas na ISO/IEC 27001 e é organizada de forma a contribuir para uma implementação satisfatória da segurança da informação, sendo baseada numa abordagem da gestão do risco. Ainda assim, a norma não apresenta nenhuma metodologia para a gestão do risco da segurança da informação (NP ISO/IEC 27001 2013; NP ISO/IEC 27005 2008).

4.2. Conformidade da norma ISO 27001 com o RGPD

Os autores Clements e Milton (2018), afirmam haver equiparações entre o RGPD e a ISO/IEC 27001. Se, por um lado, o RGPD (UE), declara que as organizações devem exercer políticas, procedimentos e processos apropriados para proteger os dados pessoais, por outro, a série da ISO/IEC 27001 adota "um conjunto de padrões de segurança da informação que fornecem recomendações de melhores práticas para a gestão da segurança da informação" (Clements and Milton 2018).

Essa norma internacional de segurança da informação, "fornece um excelente ponto de partida para alcançar os requisitos técnicos e operacionais necessários para reduzir o risco de uma violação". No entanto, como estipulado no regulamento, nem todos os dados são protegidos pelo RGPD, pois são aplicáveis apenas a dados pessoais (Lopes, Guarda, and Oliveira 2019).

Para Diamantopoulou, Tsohou, e Karyda (2019), "a série de normas ISO 27001 pode constituir uma base útil para as empresas desenvolverem as suas estratégias de conformidade, lidando com tópicos como a definição e a avaliação de riscos, avaliação contínua e documentação apropriada.".

Comparativamente, a "ISO/IEC 27001: 2013 e o RGPD, visam fortalecer a segurança dos dados e atenuar o risco de violações de dados, ambos exigem que as organizações garantam a confidencialidade, integridade e disponibilidade dos dados" (NP ISO/IEC 27001 2013).

A ISO/IEC 27001:2013 fornece boas práticas detalhadas, enquanto que o RGPD "especifica que a adesão a códigos de conduta e certificações aprovadas podem ser usadas como um elemento para demonstrar a conformidade". Contudo, existem entre ambos o poder de intencionar a adoção da proteção de processos e dados.

Para uma possível conexão da avaliação da privacidade, foi necessário identificar que pontos da ISO/IEC 27001 foram referenciados no GDPR. Em resposta a esta constatação, Hughes e Kabir (2018), referem que à primeira vista, "existem sete áreas específicas nas quais a ISO 27001 suporta diretamente a conformidade com o GDPR.".

1. Gestão de Dados Pessoais
- Relativo à Proteção de Dados Pessoais.

2. Gestão de risco de terceiros (TPRM) [19]
- Impor direitos de acesso a dados pessoais caso possam ou não ser acedidos.

3. Processo de avaliação regular da eficácia dos controlos de segurança
- Devem ser garantidas medidas adequadas de segurança da informação.

4. Avaliação de Riscos
- Incluir listas de tratamentos sujeitos à avaliação do impacto sobre a proteção de dados.

5. Criptografia
- Incluir anonimização ou a pseudonimização nos dados.

6. Backup
- Assegurar a aplicação de normas de segurança que garantam a confidencialidade e durabilidade dos SI.

7. Notificações de Violação
- Preparar decisões em processos de notificação de violações de dados pessoais;
- Disponibilização de mecanismos de rastreabilidade e notificação.

Neste sentido, foi elaborada uma tabela (anexo 1) que mapeia o aconselhamento jurídico para atender aos requisitos do RGPD da UE. Na revisão da mesma, observa-se que os controlos da norma ISO/IEC 27001 do "Anexo A" estão no corpo principal da mesma (ISO/IEC 27001:2013). Os controlos especificados no Anexo A, estão especificados e explicados com mais detalhe na norma ISO/IEC 27002:2013, sendo esta já anteriormente referida como um padrão de diretrizes suplementares sobre os controlos de Segurança da Informação.

[19] *Third Party Risk Management*, Programas que aludem para a supervisão e a monitorização do ciclo de vida de terceiros, precisam ir além da função de compras e englobar outras partes interessadas e departamentos em toda a empresa. Disponível em: (https://assets.kpmg/content/dam/kpmg/br/pdf/2019/02/br-third-party-risk-management.pdf) (Consultado em 04-01-2020)

5. Estudo de caso: Interaction Layer

5.1. Missão, visão e objetivos

A Interaction Layer, é uma empresa dedicada a serviços informáticos, sendo o foco no Cliente determinante. Com um elevado nível de empenho, procuram sempre ir de encontro às necessidades e expetativas dos seus clientes, sempre proporcionando a mais elevada qualidade, segurança e empenho na resolução dos seus problemas, associando as mais modernas tecnologias em cada área de atuação.

De acordo com a Interaction Layer (2020), a empresa pretende ser reconhecida tanto pelos seus Clientes, de modo a ter a garantia de durabilidade e confiança, como pelo mercado em geral, contando ser uma empresa sólida, empenhada e de elevado valor para os seus parceiros de negócio.

Criada há pouco menos de seis anos, é considerada uma empresa jovem, dedicada e dinâmica, pretendendo ter ao fim de cada ano uma evolução superior a 12% em todos os departamentos associados. Para isso foram estabelecidas regras especificas para o cumprimento da sua progressão (Interaction Layer 2020):

- Dinamizar o mercado, proporcionando aos clientes as melhores soluções existentes;
- Assegurar um crescimento sustentável;
- Proporcionar formações ao mais alto nível;
- Apostar em parcerias de grande valor acrescentado a nível tecnológico;
- Ajudar os clientes a atingir os seus objetivos, seja de categoria tecnológica, qualidade ou de segurança informática;
- Garantir a saúde financeira da empresa (Interaction Layer 2020).

Ambicionam encontrar respostas alternativas aos desafios colocados por cada um dos clientes e pelo mercado em geral. Para isso contamos com a partilha de conhecimento da equipa.

5.2. Problemas identificados

Para que fosse possível proceder à realização da presente dissertação foi necessário entender o problema que se encontra na génese do tema. Este, identificado de imediato, decorre da

ausência de uma base orientadora consistente, que auxilia na necessidade de se poder vir a melhorar procedimentos relacionados com a segurança da informação, baseados na análise de riscos que podem intervir na prevenção de erros e burlas informáticas. Procurando manter a credibilidade da empresa, a auditoria será capaz de comprovar se os números apresentados pelo departamento contabilístico são realmente compatíveis com a realidade da mesma. Neste caso, são avaliados tanto os registos, as políticas de controlo, os processos contratuais e as movimentações da organização.

As orientações recebidas pelos Departamentos e o Administrador da empresa, referem que relativamente à forma de organização e estruturação dos processos, é possível que estes não estejam implantados ou realizados de acordo com a sua finalidade, assim como a dúvida referente à disposição da organização que poderá não ser a mais correta – o que dificulta a sua atuação. Deste modo, este problema é transversal a todos os clientes e colaboradores da empresa.

Nesse sentido, a Interaction Layer, merece uma urgente atenção, uma vez que, para que a certificação pela ISO/IEC 27001 avance e sejam alcançados progressos, os colaboradores têm de tomar medidas drásticas para posterior validação. Constatou-se que, só após a validação da auditoria na empresa, será possível obter uma maior precisão das observações e preencher lacunas do sucedido.

5.3. Levantamento da documentação existente

O processo de levantamento de documentação foi executado de duas formas distintas. Primeiramente, foram solicitados alguns documentos durante as entrevistas. À medida que se ia desenvolvendo os temas, foram efetuadas entrevistas, na qual englobava funcionários a responsáveis da hierarquia superior, em que se mencionavam determinados documentos e politicas de controlo, nos quais lhes era solicitado o envio por email, pedido este que sempre foi atendido quando solicitado. Uma outra forma de recolha de informação foi através de um pedido de acesso ao CRM[20] da empresa, na qual teve a finalidade de se poder analisar e entender a definição de classes dos sistemas de informações e possíveis ferramentas que automatizam as funções de contacto com o cliente. No que se refere ao critério na seleção de documentos, eram solicitados todos os documentos e politicas em que a norma ISO/IEC 27001 se baseava, nas quais em que se apoiavam para a controlo da tomada de decisão. Contudo, fazia parte de um dos objetivos da presente dissertação averiguar o que se realizava para poder

[20] *Customer relationship management* - (Gestão de Relacionamento com o Cliente).

ajudar os colaboradores a melhorarem o seu desempenho, como a sua formação, descrição de cargos de diferentes níveis hierárquicos e atribuição de responsabilidades.

Durante o processo, foram realizados por motivos de simplificação, observações a elementos que correspondem às evidências físicas que foram recolhidas através da observação direta. As observações foram efetuadas durante os dias da recolha dos dados e nas realizações de entrevistas, através de uma visita guiada à instalação localizada no Porto.

Observou-se o espaço do estabelecimento, e deparou-se com a exposição de informação que é feita através de documentos e "mensagens" que são afixados em locais visíveis.

5.4. Mapeamento de fluxos de informação

Primeiramente, para a representação da informação organizacional, adotou-se a elaboração de um organograma tradicional, que, tal como o próprio nome indica, remete-se a ideia de que as estruturas empresariais seguem uma linha mais tradicional, hierárquica e, de certa forma, mais rígida e clara.

No entanto, quanto maior for o grau de autonomia e a responsabilidade exigida pelo departamento correspondente, maior será o nível dessa posição no organograma. As representações das posições refletem-se através de retângulos distribuídos de forma vertical, interligados por linhas condutoras, que representa a comunicação entre os diversos cargos e setores existentes.

Conforme referido pelo CEO da empresa, ainda que haja comunicação na hierarquia entre a administração e os restantes departamentos, existem cargos onde a pessoa que exerce as funções de administração, é também responsável por outros departamentos, o que pode complicar o controlo do fluxo da informação. Porém, o proprietário da empresa acredita que nada nos departamentos se complica, sendo autónomos em cada responsabilidade da área.

Normalmente a comunicação é descendente (de cima para baixo) e o fluxo segue desde o diretor, nomeadamente o Departamento inicial, a Administração até aos diversos subdepartamentos que referenciam os serviços encaminhados dos colaboradores.

De acordo com a Administração, esta refere que todas as informações partem da área comercial, e seguem um único caminho: Administração, Departamento Administrativo, Comercial, reencaminha para o departamento correspondente da área de serviço a desenvolver

e finaliza com o departamento financeiro. Demonstra-se na figura 4, o organograma da empresa em questão, com o fluxo das informações da mesma.

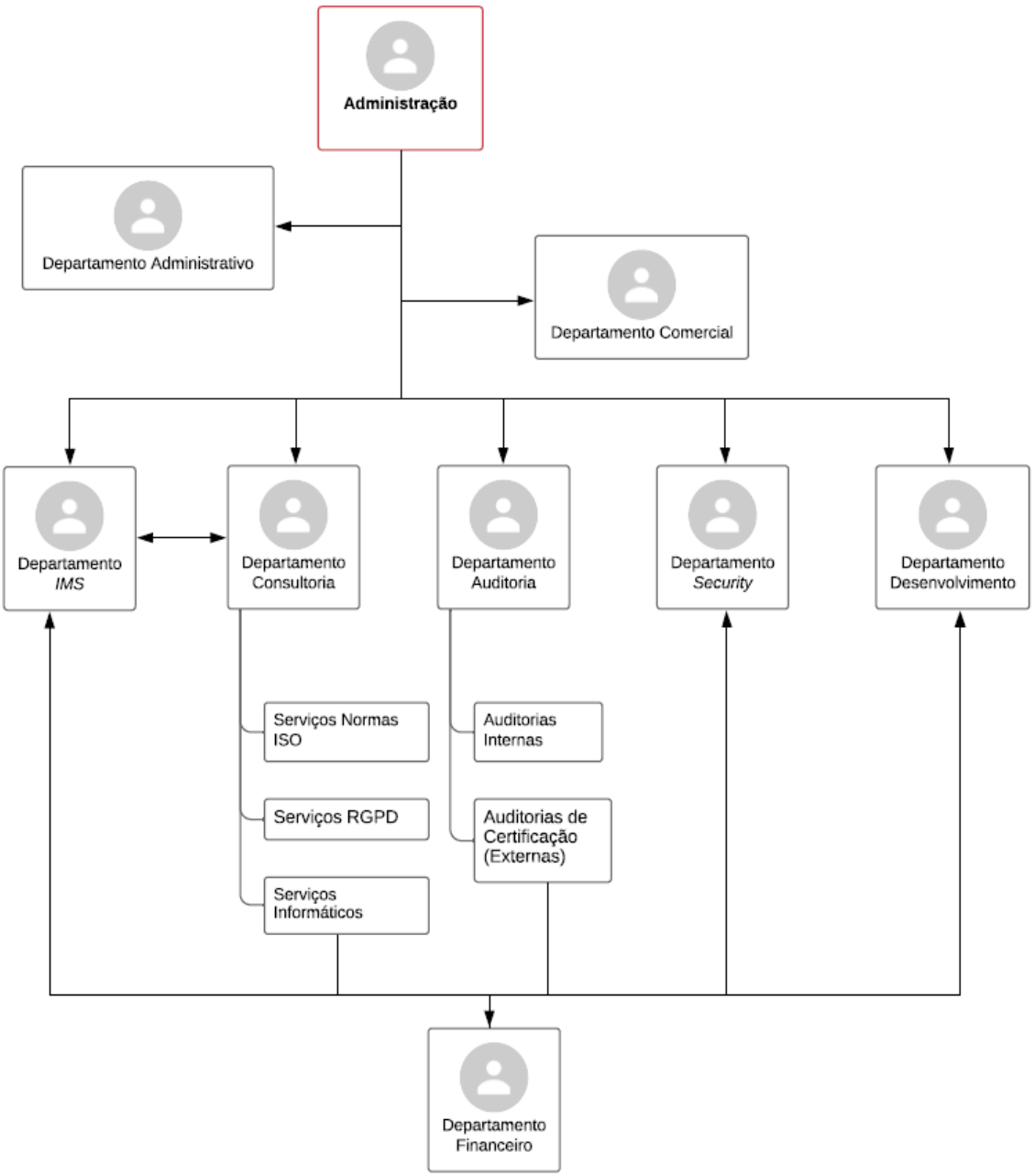


Figura 4 - Organograma Empresa Interaction Layer

Fonte: Elaboração própria

Como descrito anteriormente, existem 8 departamentos, nomeadamente e por ordem hierárquica a Administração, Departamento Administrativo, Departamento Comercial, as áreas correspondentes aos Departamentos de *IMS*, Consultoria, Auditoria, Desenvolvimento, *Security* e finaliza no Departamento Financeiro.

Primeiramente, a **Administração** tem como principal função trazer os melhores possíveis resultados organizacionais, adotando a prática da gestão com base em resultados e maximizando a possibilidade do crescimento da empresa, da sua eficácia e do seu lucro/ganho. Os funcionários referentes a este departamento devem desempenhar pelo menos quatro funções básicas de gestão, como demonstrado na figura 5:

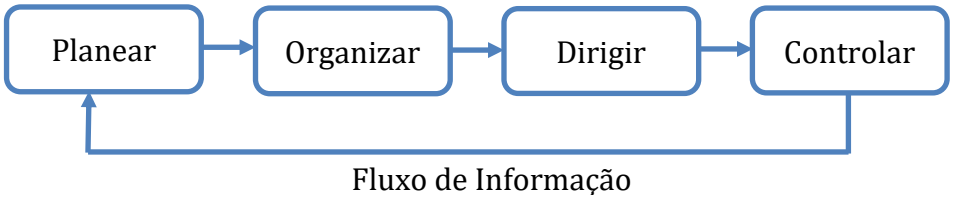


Figura 5 - Fluxo de Informação da Administração

Fonte: Elaboração própria

É fundamental que a gestão siga estes princípios de administração, acoplada por uma sigla, a PODC reúne as palavras Planear, Organizar, Dirigir e Controlar.

Entendemos assim que o conceito de administração é amplo, englobada por todos aqueles que possuem alguma responsabilidade por resultados dentro de uma organização.

A organização como função administrativa adota as funções de planeamento, com a finalidade de atingir objetivos e metas da empresa. Capaz de liderar e motivar os funcionários, organizar recursos materiais, realizar o controlo financeiro do negócio e controlar fluxos de tarefas e projetos.

Das funções com maior responsabilidade, administra e gere toda a organização, sendo responsável pela estabilidade de todos os departamentos. No seu patamar atual, correspondem objetivos vastos como realização de Budget[21], gerir finanças, entradas e saídas, além de gerir os requisitos de atividades dos departamentos.

[21] Plano financeiro por um período definido, geralmente um ano. Também pode incluir quantidades de recursos, custos e despesas, ativos, passivos e fluxos de caixa. Empresas, governos, famílias e outras organizações o utilizam para expressar planos estratégicos de atividades ou eventos em termos mensuráveis. Disponível em: (https://en.wikipedia.org/wiki/Budget) (Consultado em 10-02-2020)

Cada vez que existe uma reunião com os clientes no estabelecimento da empresa, concebe-se, dependendo da área de atuação do serviço, um representante do mencionado departamento. Caso contrário, será realizada a reunião com um representante do departamento administrativo, no qual se irá dirigir às reuniões para a recolha e estipulação de requisitos.

Hierarquicamente abaixo encontra-se o **Departamento Administrativo**, área responsável por concentrar funções de outros departamentos, como os recursos humanos ou as finanças. Área abrangente cumpre funções como sendo encarregue dos serviços externos e internos da empresa, calendarização, organização das agendas de forma a que tudo esteja coordenado e estabilizado conforme o ideal, para que não haja complicações ou ausência de informação/colaboradores.

Atua como uma parte de liderança nos setores da empresa, e a interação entre clientes. Esta relação depende do tipo de negócio e a maneira como os setores são estruturados de maneira a que os processos aconteçam. Algumas das funções mais comuns desta área, envolvem a gestão e desenvolvimento de recursos humanos, administração de produção e serviços, gestão de tesouraria, compras, vendas e cobranças, tal como o controlo do sistema de qualidade da empresa.

O **Departamento Comercial** apresenta um caráter estratégico da empresa, retém iniciativas precisam estar alinhadas ao mercado e aos objetivos e metas que se pretendem alcançar. A gestão comercial trata de entregar todos os recursos necessários para que os departamentos correspondentes aos serviços e ao financeiro tenham condições de trabalhar. Ou seja, pode-se atribuir a gestão comercial à ideia de uma "administração" otimizada do departamento administrativo, tecnológicos e financeiros de uma organização, com o intuito final de entregar a todos os envolvidos — acionistas, colaboradores e clientes — os melhores resultados (figura 6).

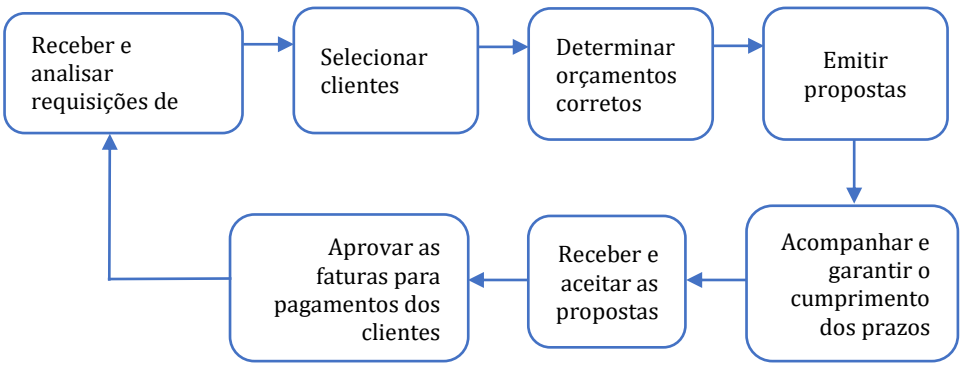


Figura 6 - Fluxo de Informação Departamento Comercial

Fonte: Elaboração própria

Na Interaction Layer, o Departamento Comercial garante que a empresa e os seus serviços estão competitivos no mercado, porém, motiva-se com o aumento da produtividade na empresa, responsável pela venda e estabelecimento de contactos, estabelecimento de propostas e manutenção dos clientes após adoção do serviço, como a atualização de registos e a necessidades dos clientes.

5.4.1. Análise e modelação de processos

O mapeamento de processos considera-se uma ferramenta de gestão primordial, que tem como objetivo identificar, o fluxo de informação, as partes envolvidas, capacidades, competências e recursos para responder a todos os componentes que sejam necessários. Desse modo, é capaz de fazer com que todas as atividades de uma empresa/negócio tenham o objetivo inicial, com a organização e estruturação adequada, suprimindo complicações desnecessárias.

De acordo com a análise do processo comercial, é demonstrado na figura 7, o fluxo de informação correspondente às atividades exercidas no departamento comercial.

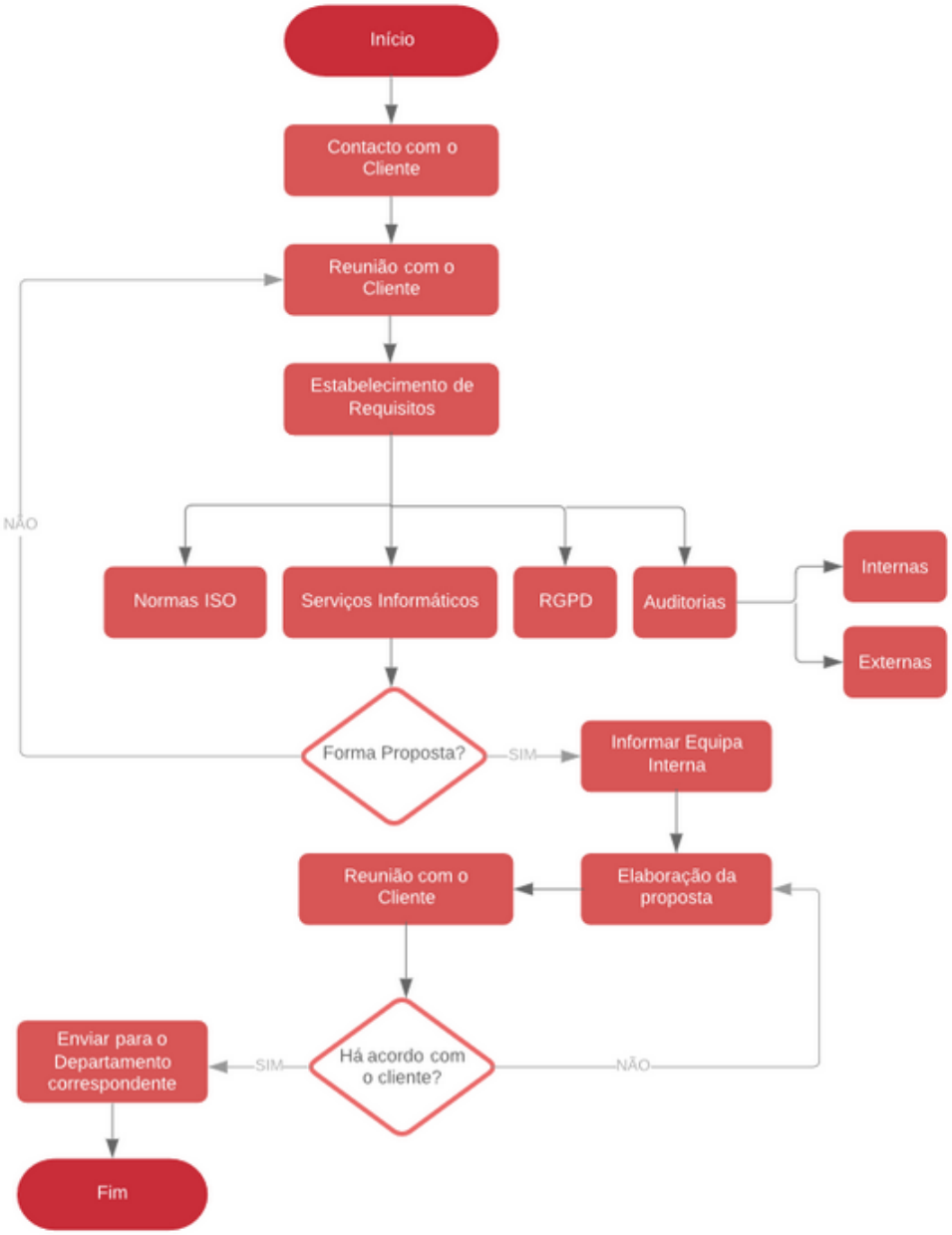


Figura 7 - Mapeamento do Processo Comercial

Fonte: Elaboração própria

Posteriormente, será enviado o serviço ao departamento correspondente. Na Interaction Layer existem quatro departamentos existentes para a realização de serviços, nomeadamente o Departamento de Consultoria, Departamento de Auditoria, Departamento *IMS* e o Departamento *Security*.

Relativamente ao **Departamento de Consultoria**, este desenvolve ações relacionadas com a prestação de serviços integrados de consultoria, como normas, consultoria e RGPD e serviços

IT. Este último serviço engloba o desenvolvimento de software de apoio à gestão, em todas as áreas de que as entidades necessitem. Além do fornecimento dos serviços referenciados, desenvolvem também estudos estratégicos e estudos de mercado, diagnósticos e análises de necessidades, planos estratégicos e outros estudos ou propostas solicitadas pelos clientes, porém são responsáveis pela calendarização correspondente às propostas impostas pelos mesmos.

Assim que é requerido um pedido da área de Consultoria na especialidade de "Normas ISO", existe primeiramente uma 1.ª reunião com o cliente, na qual será identificado o objetivo principal e recolha de informações que sejam necessárias para a criação do processo interno. Posteriormente é emitida uma proposta ao cliente que pode ou não ser aceite.

- Caso a proposta não seja aceite:
    - Verifica-se através de uma 2.ª reunião junto do potencial cliente, qual terá sido o motivo da negação, de forma a poder eventualmente melhorar o processo e identificar as ações a implantar, e caso seja aplicável elaborar uma revisão à proposta.

- Caso a proposta seja aceite:
    - Define-se uma equipa interna que irá tomar conta de todo o projeto, informando o cliente de eventuais resultados e informações.

Assim que o projeto é finalizado, é efetuada através de uma reunião, uma análise (com o cliente) sobre os aspetos que se poderão vir a melhorar e a avaliação que a prestação da equipa que esteve envolvida no projeto. A consentida análise servirá para melhorar as equipas, o serviço, e principalmente, avaliar a prestação deste serviço.

Contudo, existem fulcrais documentos e ações que devem ser adotadas para este procedimento, como o *Roadmap* de todas as atividades, reuniões regulares com o cliente e a equipa interna envolvida, a criação da documentação inicial ao desenvolvimento do projeto e a elaboração de atas de reuniões que são distribuídas pelos iminentes colaboradores do projeto.

Na Interaction Layer foi desenvolvido, no sentido de aprofundar este processo, a criação de um "Procedimento PRO", que contém todas as informações e documentos a criar face a um Projeto de alto nível de Consultoria.

O serviço prestado de especialidade RGPD, é em toda a sua essência igual ao fluxo responsável pela “Normas ISO”, mas o que as difere é a sua finalidade. O objetivo primordial desta área é validar a adequabilidade da empresa na conformidade com o regulamento geral da proteção de dados, em toda a sua plenitude. Os dois serviços encontram-se representados no fluxo da figura 8.

Em terceira e última especialidade, encontra-se o serviço de consultoria informática, que abrange conteúdos relativos ao estudo e à infraestrutura existente nas empresas, aconselhamento para mudar a infraestrutura, desenvolvimento aplicacional, além de caso seja de vontade do cliente, uma prestação associada a um serviço de *security*, responsável pelo **Departamento *Security***. Por esse mesmo motivo, o fluxo dos anteriores torna-se diferente na medida em que existe a exceção de uma “saída” para os processos *security*, demonstrado nas figuras 8 e 9.

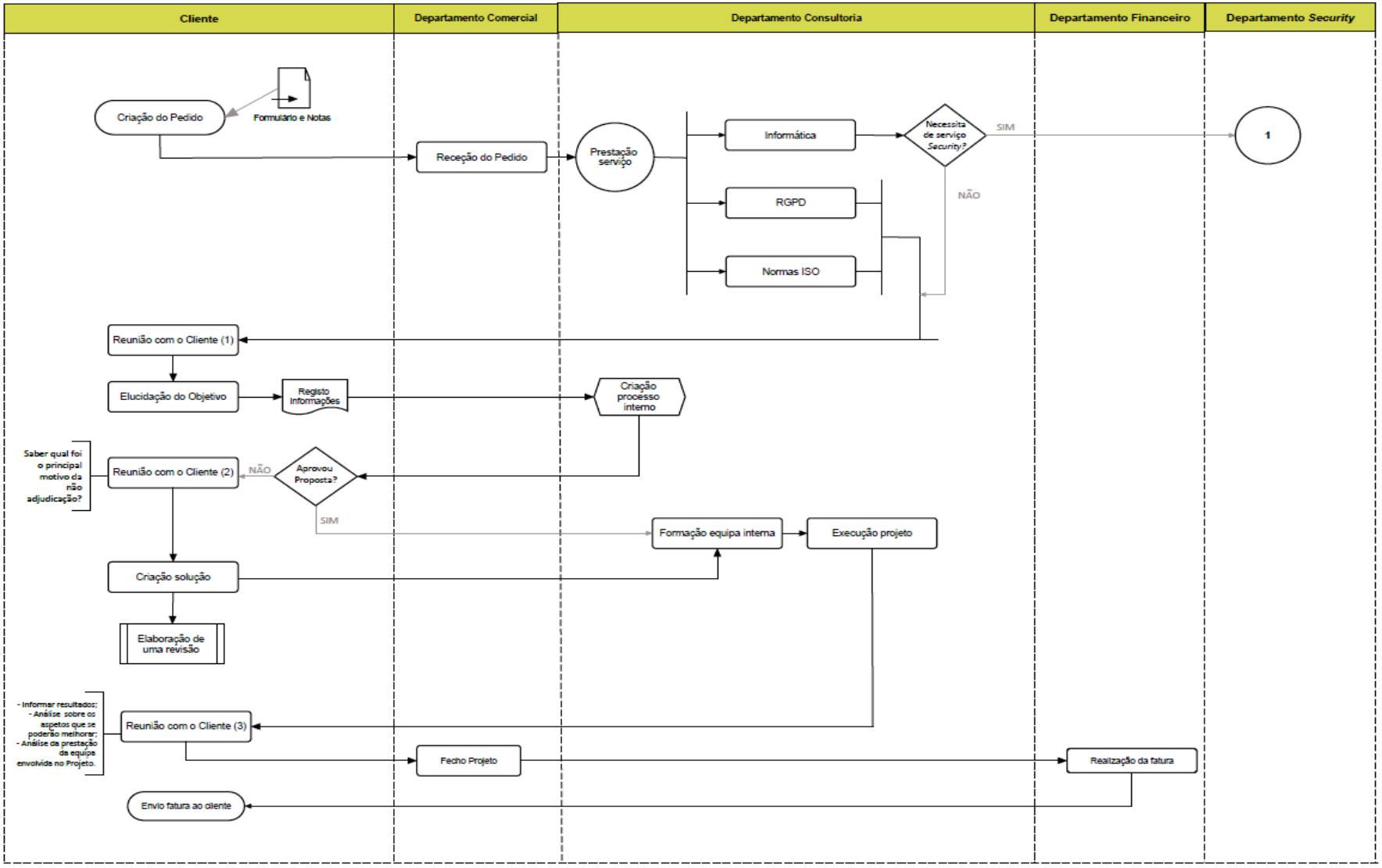


Figura 8 - Mapeamento do Processo Consultoria1
Fonte: Elaboração própria

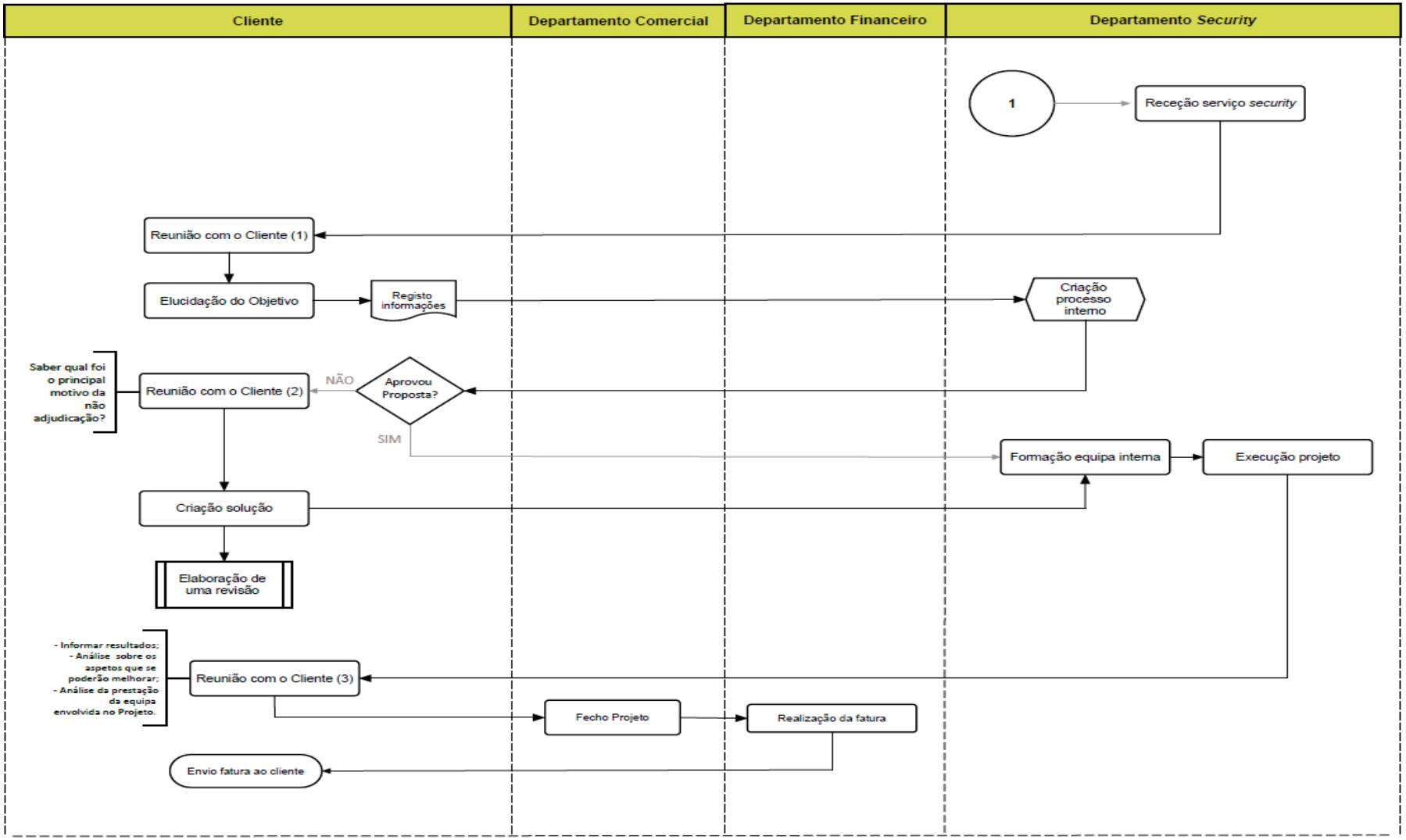


Figura 9 - Mapeamento do Processo Consultoria2

Fonte: Elaboração própria

O **Departamento de Auditoria** tem como finalidade, realizar planos de desenvolvimento, que auxiliem a empresa a alcançar os seus objetivos, adotando serviços de forma estruturada e disciplinada para a avaliação e aperfeiçoamento da eficácia dos processos de gestão de riscos com o objetivo de acrescentar valor, assim como melhorar as operações e resultados que adotou do serviço à empresa a auditar. Obviamente, como todos os departamentos, esta presta ajuda à Administração e desenvolver adequadamente suas atribuições, proporcionando-lhes análises, recomendações e comentários objetivos, acerca das atividades examinadas.
O Departamento de Auditoria é subdividido em duas categorias:

a) Auditoria Interna: Trabalho solicitado pelo cliente, que chega à empresa Interaction Layer através da área do Departamento Comercial e tem como objetivos:

    a. Validação de processos;
    b. Procedimentos e instruções de trabalho mediante os requisitos através das normas ISO/IEC 9001; ISO/IEC 20000; ISO/IEC 22301; ISO/IEC 27001; ISO/IEC 31000 e normas associadas ao RGPD.

    Posteriormente, são realizadas como preparação de uma auditoria externa ou unicamente como teste ao sistema.

Após a receção do pedido de auditoria interna pelo Departamento Comercial, é informado o Departamento de Auditoria e é atribuída uma data de acordo com a disponibilidade da equipa auditora da empresa Interaction Layer, sendo a data imediatamente proposta ao cliente. Em caso de aceitação a auditoria é marcada. Caso a data proposta não seja aceite por parte do cliente, é proposta uma nova data.

Na data marcada é feita a auditoria interna e no final da mesma é emitido um relatório *onsite* e o mesmo é dado a conhecer ao cliente na reunião de fecho da auditoria.

No caso de existirem "não conformidades" mais complicadas, o processo fica em estado "aberto" por parte do Auditor Coordenador até haver resposta às mesmas identificadas na auditoria interna por parte da empresa auditada.

Após a receção da(s) resposta(s) às "não conformidades" (mais complicadas) por parte da empresa auditada, esta(s) é(são) analisada(s) pelo Auditor Coordenador e caso as respostas sejam aceites, o processo é fechado e a informação facultada à empresa auditada.
Posteriormente à execução do serviço, é enviada a fatura para a empresa cliente pelo **Departamento Financeiro** (figura 10).

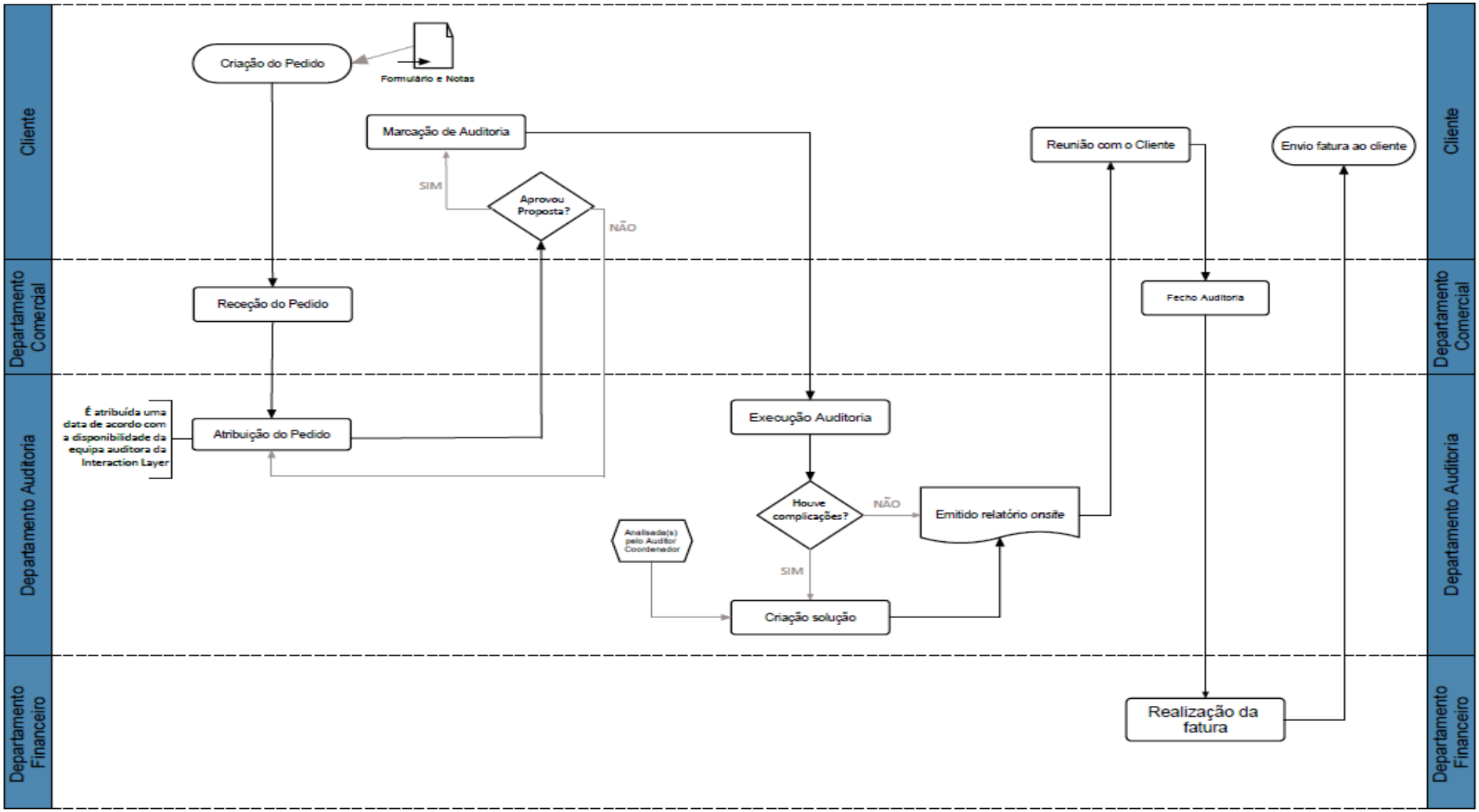


Figura 10 - Mapeamento do Processo Auditoria Interna

Fonte: Elaboração própria

b) Auditoria Externa: Consideradas auditorias de 2.ºgrau, são auditorias que têm como objetivos:
   - Averiguar o cumprimento de todos os requisitos das normas (ISO/IEC 9001 e ISO/IEC 27001) com a finalidade de certificar uma empresa[22];
   - Averiguar documentos jurídicos com a finalidade de certificar uma empresa.

   Esta categoria de auditoria, é realizada por uma entidade certificadora.

Após a receção do pedido de auditoria externa pelo Departamento Comercial, é informado ao Departamento de Auditoria e é atribuída uma data de acordo com a disponibilidade da equipa auditora da empresa Interaction Layer, sendo a data imediatamente proposta ao cliente. Em caso de aceitação a auditoria é marcada. Caso a data proposta não seja aceite por parte do cliente, é proposta uma nova data.

Antes da data marcada, a equipa auditora deve ter acesso à documentação da empresa que vai auditar de forma a preparar a auditoria, é feito o plano da auditoria que é disponibilizado ao Cliente e à entidade certificadora.

Na data marcada é feita a auditoria externa e no final é emitido o relatório *onsite* e o mesmo é dado a conhecer ao cliente na reunião de fecho da auditoria. No caso de existirem "não conformidades" mais complicadas, o processo fica em estado "aberto" por parte do Auditor Coordenador até haver resposta às mesmas identificadas na auditoria interna por parte da empresa auditada.

Após a receção da(s) resposta(s) às "não conformidades" (mais complicadas) por parte da empresa auditada, esta(s) é(são) analisada(s) pelo Auditor Coordenador e caso as respostas sejam aceites, o processo é fechado e a informação facultada à empresa auditada.
Posteriormente à execução do serviço, é enviada a fatura para a empresa cliente pelo Departamento Financeiro (figura 11).

[22] A Interaction Layer pertence à Bolsa de Auditores de uma empresa Multinacional de renome e com formação administrada pelo *IRCA* (*International Register of Certificated Auditors*)

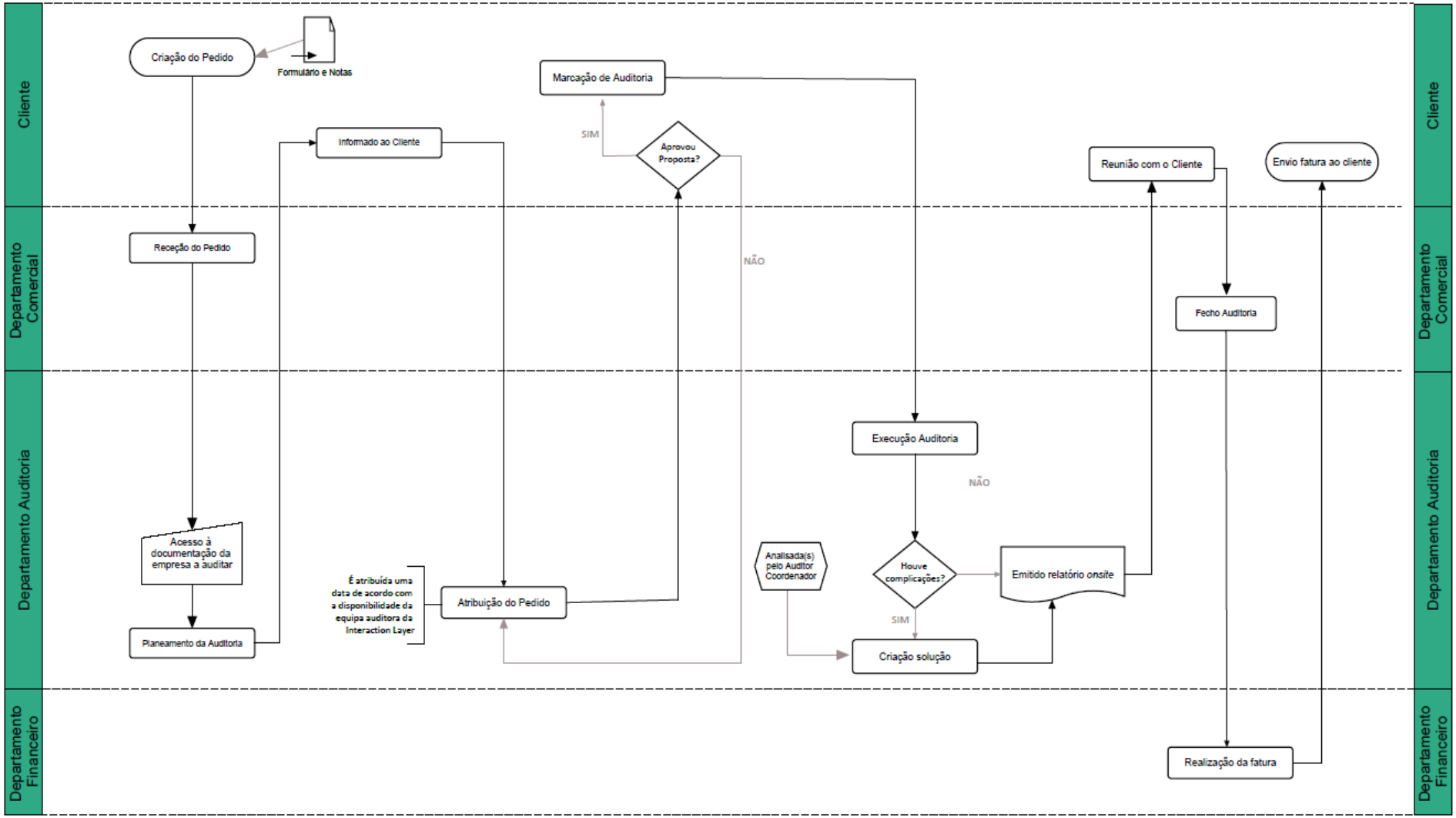


Figura 11 - Mapeamento do Processo Auditoria Externa

Fonte: Elaboração própria

Relativamente ao **Departamento Financeiro,** já referido anteriormente, tem o objetivo de lidar com questões relacionadas com a administração de recursos da empresa. Tem a responsabilidade de controlar tudo aquilo que se associa a custos (tesouraria), faturação dos trabalhos realizados, contabilidade, controlo de contas a pagar e a receber, investimentos, gestão dos impostos, além do planeamento financeiro e divulgação dos resultados para os investidores.

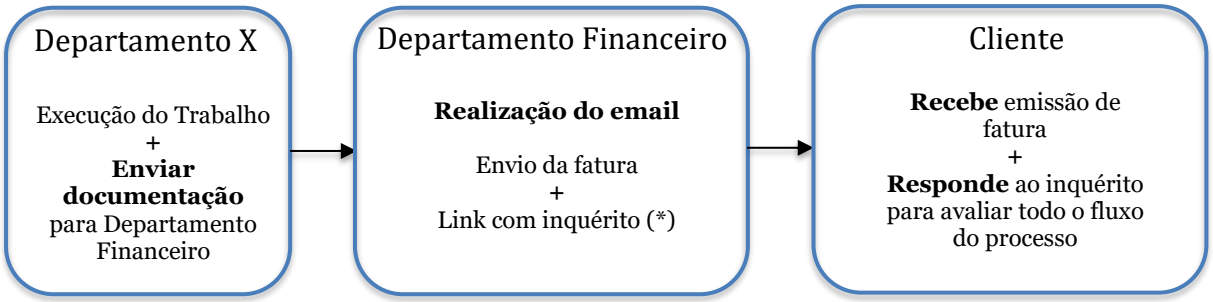
Encarrega-se de garantir os recursos necessários para que a empresa possa cumprir os seus princípios, de modo a manter-se competitiva e ativa, garantindo lucros imediatos e a longo prazo.

Setor aplicável a todos os outros departamentos da empresa pelo controlo diário das entradas e saídas de dinheiro, realizado este de modo eletrónico. A gestão de contas a pagar controla o vencimento de contas de consumo e pagamento de fornecedores, a fim de evitar multas e atrasos. Responsável também pelo controlo dos salários mensais, verificando diariamente se os clientes estão em dia com as suas obrigações, se a empresa emitiu pagamentos fora de prazo e, caso seja necessário, implementar mecanismos de obrigação.

Realização do pedido de faturação:

- Posteriormente à execução do trabalho de cada departamento, deve ser obrigatoriamente dada a indicação ao Departamento Financeiro a remessa da faturação, para realização da emissão da fatura, de acordo com os valores estabelecidos na proposta.
- Os pedidos da faturação podem ser de prazo mensal, caso o trabalho seja de longa duração (mais de um mês).
- No software CRM, deve estar diariamente atualizada a proposta e o consentimento com o valor correto a faturar.
- O envio de informações, como valores a faturar, devem ser transmitidos ao Departamento de financeiro através de correio eletrónico.

Envio da Fatura ao Cliente:



(*)
- Avaliar as reuniões;
- Avaliar as equipas que participaram no projeto;
- Analisar pontos de melhoria;
- Analisar pontos fracos;
- Satisfação global

Figura 12 - Processo envio fatura ao Cliente

Fonte: Elaboração própria

O **Departamento de Desenvolvimento,** é responsável, tal como nome indica, pela área de especialização na execução de trabalhos de desenvolvimento relativo a novas soluções de software. Essa identificação de oportunidades no desenvolvimento de novas soluções de software surge através de possíveis solicitações por parte de clientes e na análise de necessidades e expetativas do mercado.

Em associação a este setor da empresa, existem diversas atividades básicas comuns à grande parte dos processos existentes:

- Levantamento de requisitos (conhecer as necessidades do cliente e definir os requisitos);
- Análise de Requisitos (avaliar a viabilidade do projeto);
- Projeto (documentar procedimentos e desenvolvimento da metodologia e projeto);
- Implementação (através de reuniões transmitir ao cliente e implementar o desenvolvido);
- Testes (testar as funcionalidades desenvolvidas);
- Implantação (fase final do projeto/fecho de projeto).

Contudo, a Interaction Layer preza pelos custos do cliente e da empresa, na medida em que todas as equipas dos departamentos desenvolvem e analisam os seus projetos conforme a identificação da competitividade, garantindo princípios de qualidade à menor despesa. Pensando no custo como um todo, a empresa assevera pontos fulcrais neste setor:

- ✓ Aprimoração de novas soluções, com a finalidade inalterável por um preço menor. Garantindo uma ação vantajosa para o cliente;
- ✓ Reaproveitamento de *frameworks* e códigos para outros projetos;
- ✓ Saber quais as tecnologias que poderão vir a ser usadas (base de dados, plataforma de backups como *clouds*, linguagens de programação).

Na figura 13, explica-se através de um fluxograma, que a execução de um projeto, define-se em várias fases. Primeiramente, a equipa da Interaction Layer*,* responsável pelo projeto de desenvolvimento de software necessita de recolher e validar com o cliente os requisitos necessários antes de dar início a qualquer etapa de produção. Esta é considerada uma etapa primordial para se definir a gênese, através de diversas reuniões, pelas quais a equipa posiciona as informações recolhidas e as traduz para uma linguagem técnica (tipo de meio de comunicação pertencentes a áreas específicas do conhecimento humano).

Após a receção de toda a informação, é necessário avaliar a viabilidade do presente projeto, e realizar uma elaboração de uma especificação técnica e funcional, com a descrição de todas as características do software e se a mesma permite avaliar se as informações estão de acordo com o que foi realizado na fase da recolha de requisitos. Logo após a esse processo, segue-se para o início da execução do processo de desenvolvimento.

Posteriormente, as funcionalidades do projeto são novamente validadas com o cliente e, caso não haja aprovação da mesma, o software é implantado ou atualizado e instalado na empresa do cliente.

Por último temos a fase direta para o Departamento Financeiro, relativamente ao fecho do projeto e emissão da faturação.

Nota: Entre as fases que ajudam a manter a qualidade no desenvolvimento de softwares estão testes regulares da ferramenta, revisão de códigos e a organização de uma equipa voltada para descobrir possíveis problemas nos sistemas e processos.

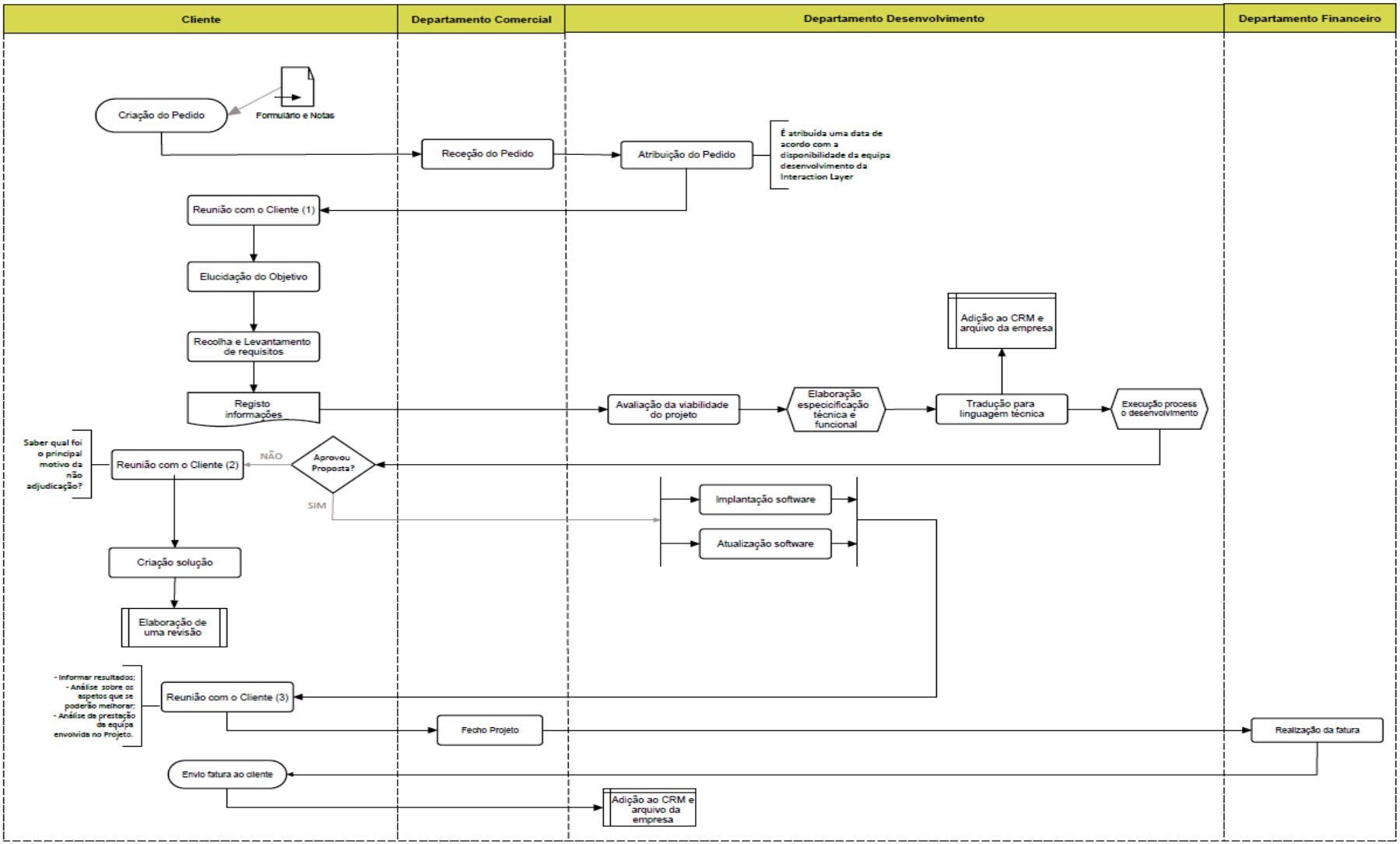


Figura 13 - Mapeamento do Processo Desenvolvimento

Fonte: Elaboração própria

Os profissionais pertencentes ao mundo dos negócios, estão atualmente em constante mudança e devem ser capazes de ter habilidades e especializações precisas e distintas, permitindo que estes mostrem os seus únicos talentos que os diferenciem dos outros. Com isso o último departamento que se menciona é bastante específico.

O **Departamento IMS** (*Information Management System*)**,** é o departamento responsável por definir acompanhar toda a informação existente na empresa na vertente da norma ISO/IEC 27001 e do RGPD. Porém, é o setor encarregado do estudo da gestão de sistemas de informações em diversos negócios.

O termo conhecido como gestão de sistemas de informação, fornece aos colaboradores e responsáveis da empresa relatórios, funções de planeamento, controlo e tomada de decisão e, frequentemente, acessos on-line ao desempenho atual da organização. Normalmente, os colaboradores deste departamento são orientados quase exclusivamente para eventos internos ou externos.

Os colaboradores do IMS ajudam as empresas a obter o máximo benefício do investimento em pessoal, visto ser um campo orientado para a proteção da informação das pessoas, com ênfase no serviço por meio da tecnologia. As empresas usam sistemas de informação em todos os níveis de operação para coletar, processar e armazenar dados. Ao trabalhar em colaboração com várias entidades especialistas na área e equipas de trabalho, bem como os seus clientes, os profissionais da IMS desempenham um papel fundamental nas áreas como a segurança da informação, proteção de dados e negócios de integração (figura 14).

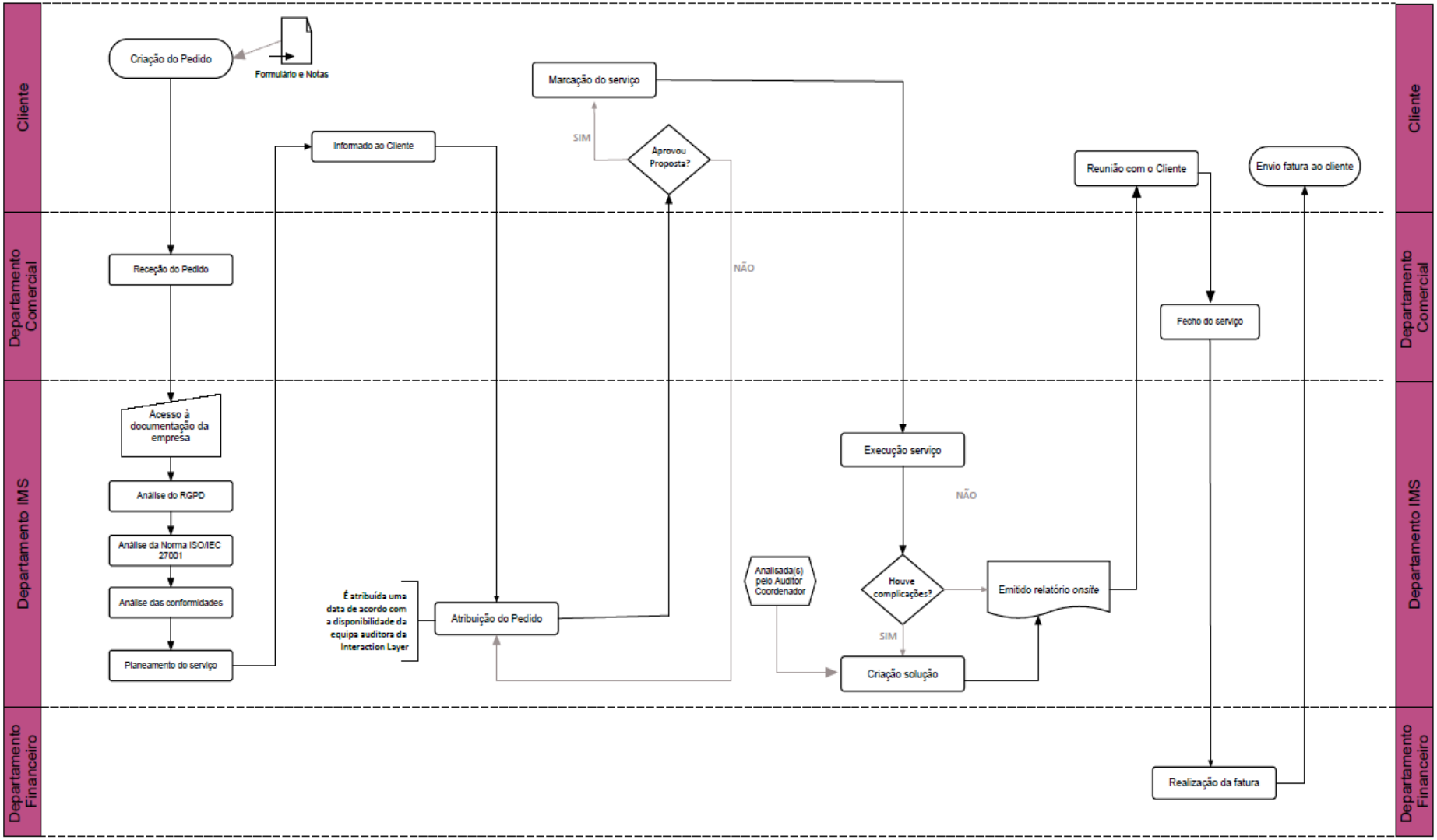


Figura 14 - Mapeamento do Processo IMS

Fonte: Elaboração própria

5.5. Aplicação da norma aos processos de negócio da Interaction Layer

5.5.1. Verificação e análise de ameaças

Na avaliação da norma, foram levantadas ameaças que afetam diretamente os ativos da empresa IL. A análise desta fase foi efetuada de acordo com as diretrizes da norma ISO/IEC 27005 e os riscos associados na mesma (Anexo 2). Os mesmos apuram-se em vulnerabilidades e ameaças, que podem causar a perda da confidencialidade da informação.

Como referido anteriormente, a análise ao conhecimento e registo das ameaças a que os ativos estão suscetíveis, que para esse feito optou-se pela norma 27005 que dá diretrizes sobre o risco a que os mesmos estão sujeitos. Porém, na respetiva norma encontram-se anexos que demonstram as vulnerabilidades e origens dos riscos.

É de extrema necessidade o desenvolvimento de uma listagem de ameaças específicos e possivelmente detetados no respetivo âmbito empresarial. Porém não é mencionado requisitos correspondentes ás dimensões dos riscos, como demonstrado na tabela 5.

No entanto para a realização das tabelas, foi necessário recolher informação pertinente e especifica de empresas que desenvolvem serviços no mesmo setor que a Interaction Layer. Porém, após uma breve contextualização de vários artigos e análises, foi possível observar que, as atualizações evidentes nas empresas de consultoria informática divergem e eventualmente cada empresa funciona de forma diferente. Ainda assim, foi possível reconhecer que as mesmas se realizam entre intervalos do primeiro ano até numerosos anos.

A mesma tática serve de exemplo para a tabela de impacto causado (tabela 6), devido à diversidade de consequências que podem acarretar numa empresa. A variedade de perda de lucro varia de cêntimos a danos irreversíveis que podem levar uma empresa ao seu fecho.

Para a sua análise foi necessária uma escala, definidos assim escalas de valores numéricos, em que:

- Probabilidade: Quanto maior for a probabilidade de ocorrência, maior a sua classificação (tabela 5).
- Impacto: Referente aos danos que se verificam, quanto maior for o impacto, maior é a sua classificação (tabela 6).

Classificação	Probabilidade de ocorrer
1	1x em 10 000 anos
2	1x em 1 000 anos
3	1x em 100 anos
4	1x em 10 anos
5	1x em 1 ano
6	1x no 1 mês
7	1x na semana
8	1x por dia
9	1x por hora
10	1x por minuto

Tabela 5 - Grau de Probabilidade

Fonte: Elaboração própria

A análise definida para o risco associa-se à estimativa da probabilidade de o mesmo ocorrer com o impacto derivado.

Classificação	Impacto causado (dano)
1	< 1 euro *(*)*
2	1 euro
3	10 euros
4	100 euros
5	1 000 euros
6	10 000 euros
7	100 000 euros
8	1 000 000 euros
9	10 000 000 euros
10	Danos absolutos *(**)*

(*) Atuação não prioritária
(**) Atuação muito urgente, requerendo medidas imediatas

Tabela 6 - Grau de Impacto

Fonte: Elaboração própria

Na avaliação dos riscos foi definido um modelo de Matriz (Matriz de Risco), essencial para avaliar os resultados das análises do levantamento dos riscos.

Impacto / Probabilidade	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

Tabela 7 - Matriz de Risco

Fonte: Elaboração própria

A matriz referida na tabela 7 representa o cruzamento dos resultados de ambos os graus (Probabilidade / Impacto), facilitando deste modo a identificação dos níveis de risco presentes:

- Riscos de Baixo Nível
  - Cor: Verde;
  - Escala: 1 a 6
- Riscos de Médio Nível
  - Cor: Amarelo;
  - Escala: 7 a 8
- Riscos de Alto Nível
  - Cor: Vermelho;
  - Escala: 9 a 10

Importante ressaltar que, a cada nível de risco foi definido um prazo/período de tempo que fosse adequado para a sua resolução, assim como a mediação de prioridade a estabelecer inicialmente. No entanto, é necessário comunicar rigorosamente as mesmas à Administração da empresa para posterior aprovação. Por esta circunstância, o exemplo de um cenário numa empresa, em que existe uma restrição a nível orçamental que acarrete o adiamento da

inserção de medidas de segurança, vai de encontro à norma ISO/IEC 27001 de acordo com a responsabilidade pela informação, encarregue à administração.

Nível de Risco	Mediação de prioridade	Período de tempo
Baixo	Não prioritária *(*)*	3 a 6 meses
Médio	Necessária marcação *(**)*	1 a 2 meses
Alto	Prioritária	Ação imediata

(*) Médio-prazo
(**) Curto-prazo

Tabela 8 - Mediação de prioridade e período de tempo

Fonte: Elaboração própria

A intervenção de cada risco é fulcral para o processo de resolução, devendo ser prioritário não só os riscos mais iminentes, mas também aqueles que são mais facilmente executados, sendo o período de tempo previsto consoante com a mediação de prioridade (tabela 8).

Cumprindo o ciclo PDCA, a cada teste realizado deve-se produzir resultados verídicos e comparáveis, dado que será necessário revisar os riscos periodicamente (apenas em casos que as propostas aparentem ter mudanças significativas ou quando as mesmas ocorrem). No entanto, para cada risco que não seja aceite, é necessário aplicar um ou mais controlos do Anexo A, associado à norma ISO/IEC 27001:2013, executando novamente as fases do ciclo, para posteriormente calcular de novo o risco após a implementação do(s) controlo(s).

Claramente o ciberespaço[23], é constituído por ameaças e incertezas, porém, a gestão de riscos ajuda a fortificar o nível de segurança nas empresas, na medida em que engloba as condições para a elaboração de um plano de tratamento de risco.

De acordo com resultado da análise de risco, esta apresenta no geral, um resultado de baixo nível. Significa isto que, alguns dos riscos que possuem valores são de níveis baixos o suficiente para serem considerados aceitáveis. No entanto, alguns dos riscos registados como as ameaças

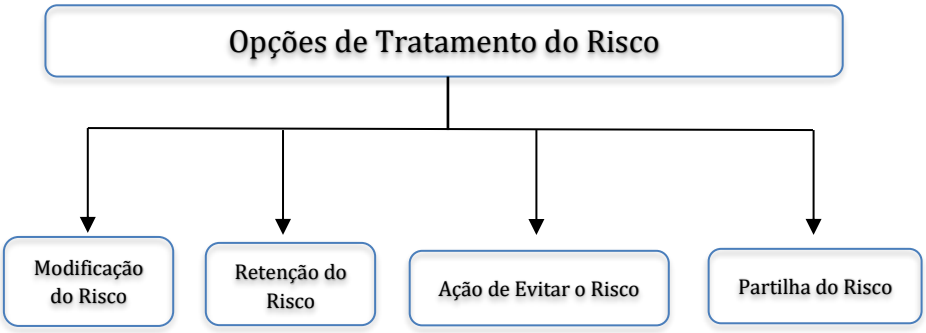
[23] "Meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações" Disponível em: (https://www.webartigos.com/artigos/o-que-e-ciberespaco/22537/) (Consultado em 02-04-2020)

de danos físicos ou o comprometimento de funções e de informação, terão de ser revistos para serem recolocados num nível considerado aceitável.

5.5.2. Plano de tratamento de risco

A norma ISO/IEC 27005:2011, contém uma lista de riscos priorizados, tendo em conta os critérios de avaliação baseados nos riscos em relação aos cenários que poderão estar afetos às empresas.

De acordo com as diretrizes de implementação, existem quatro opções disponíveis para o tratamento de risco, para o seu controlo e definição de um plano de tratamento de riscos.



Nota: A ISO/IEC 27001 usa o termo "aceitação de risco" em vez de "retenção de risco"

Figura 15 - Atividade de tratamento de risco

Fonte: Elaboração própria (baseada na norma ISO/IEC 27005:2011)

Modificação do Risco

Com a implementação dos controlos de segurança, os mesmos permitem a sua correção, eliminação, prevenção, recuperação, monitorização e consciencialização.

Retenção (ou Aceitação) do Risco

Para a implementação das decisões sobre retenção do risco, é necessário que sejam tomadas medidas e controlos tendo como base a avaliação de riscos.

Ação de Evitar o Risco

Quando são identificados os riscos, analisa-se caso estes sejam altos ou os seus custos de implementação excedem o limite, podem ser tomadas medidas para evitar completamente o risco. A título de exemplo, os riscos causados pela natureza, concebem alternativas mais económicas, como mudar fisicamente as instalações do tratamento de informações para um local em que o risco não exista ou esteja sob controlo.

Partilha do Risco

O risco deve ser transferido para alguém com o devido cargo de poder monitorizar o sistema de informações e que possa suster medidas imediatas para poder prevenir ataques antes do mesmo poder causar um nível de dano.

No entanto, é importante ressaltar que o tratamento do risco consiste numa avaliação no nível de risco ser aceitável ou não. Caso o mesmo não seja aceitável será definido um novo tratamento, quando não, é realizada uma avaliação ao tratamento escolhido.

Para operacionalizar o tratamento de risco é necessária a elaboração de uma das ações do SGSI, o considerado Plano de Tratamento do Risco. O plano retrata a ameaça e o controlo utilizado, a sua descrição, detalhe da implementação e a prioridade de intervenção. Contudo, este plano apenas será mencionado após a finalização da auditoria com os levantamentos e observações da Norma ISO/IEC 27001:2013.

5.6. Realização da auditoria da norma ISO 27001

Atualmente, não se torna totalmente seguro apenas executar as normas de segurança impostas pela própria empresa. A mesma tem que provar de algum modo que as normas de segurança estão a ser cumpridas. É através da constante realização de auditorias num estabelecimento que se produzem relatórios e documentos atualizados e com melhores práticas de segurança.

No que se conclui a importância de compreender que uma auditoria de segurança é um processo constante que deve contribuir para uma melhoria contínua para qualquer empresa.

A auditoria de segurança da informação, é um processo que refere controlos específicos destinados a avaliar os riscos de segurança que uma organização ou empresa enfrenta, a avaliar as contramedidas que são empregues pela empresa de forma a diminuir esses riscos. Basicamente, uma auditoria de segurança da informação deve identificar ataques (gestão de ameaças e riscos – referido no Anexo 2) que por si constituem uma ameaça para a rede da empresa. Será também imprescindível avaliar a administração do sistema, os controlos de gestão e como alistado, a conformidade com as normas de segurança. Tem como finalidade dar uma perspetiva valiosa para futuras auditorias, dando uma visão geral e precisa ao administrador da empresa.

Efetuar uma auditoria é tipicamente um processo humano, bastante calculoso e dependendo da dimensão árduo, gerido por uma equipa de "auditores", no qual possuem elevados conhecimentos técnicos e específicos na área das TIC.

Equipas como estas, são encarregues de entrevistar todos os colaboradores da empresa, na condução de avaliações de vulnerabilidades, documentos e políticas de segurança existentes, e na análise de sistemas das tecnologias de informação, de acordo com o âmbito da auditoria.

De seguida, encontram-se exemplos de questões adequadas, na qual esta presente auditoria de segurança de informação teve a necessidade de incutir:

- Existem *logins* de acesso? Que tipo de privacidade e documentos contêm em cada departamento/colaborador? (análise de quem poderá aceder a dados confidenciais)
- A rede organizacional tem listas de controlo de acesso? Com que intensidade?
- Os computadores da empresa são regularmente verificados quanto aos antivírus?
- Quão difíceis são as passwords? Altera-se regularmente as mesmas?
- Quem tem acesso ao *backup* de ficheiros?

Atualmente, as políticas de segurança tornaram-se documentos de conteúdos e informação desatualizados, por motivos de razões secundárias numa empresa. Uma auditoria deve não só apenas avaliar o cumprimento das políticas de segurança, mas também avaliar a sua qualidade. Por esse motivo, as auditorias tornam-se fulcrais num processo de constante manutenção eficaz e definição das políticas.

Um dos grandes benefícios desta auditoria, seria identificar possíveis falhas de segurança, que possam ser descobertas a tempo e melhoradas, com a indicação de quais seriam as medidas corretivas de forma a melhorar a segurança da mesma.

5.7. Análise de resultados e recomendações

Sendo um dos objetivos da dissertação, realizou-se uma análise de resultados de implementação, apresentada na Lista de Verificação de Auditoria (Anexo 3). De acordo com a auditoria, existem 114 controlos em 14 categorias, pertencentes à respetiva norma ISO/IEC 27001:2013.

Relativamente ao estudo prático realizado, e tendo em conta a informação recolhida no decorrer das entrevistas e análise de documentação, é possível concluir que, de um modo geral, a organização executa diariamente as suas ações diárias e planos de trabalho. Com base no Anexo 2 e 3, foi-nos possível uma análise mais detalhada acerca da execução dos controlos práticos associados aos princípios, processos e políticas presentes na norma, conforme demonstrado.

Estado de Verificação dos Controlos da Norma 27001

IM	Implementado
PM	Parcialmente Implementado
NI	Não Implementado
NA	Não se Aplica

Tabela 9 - Estado de Verificação dos Controlos da Norma 27001

Fonte: Elaboração própria

Neste sentido, constatou-se a implementação parcial e incumprimento de algumas práticas pertencentes à lista, o que nos sugere, de imediato, a existência de melhorias que a organização deverá incorporar, a fim de melhorar a gestão do sistema da segurança da informação presente,

não só para o bem da organização, mas também na prestação de serviços aos clientes.

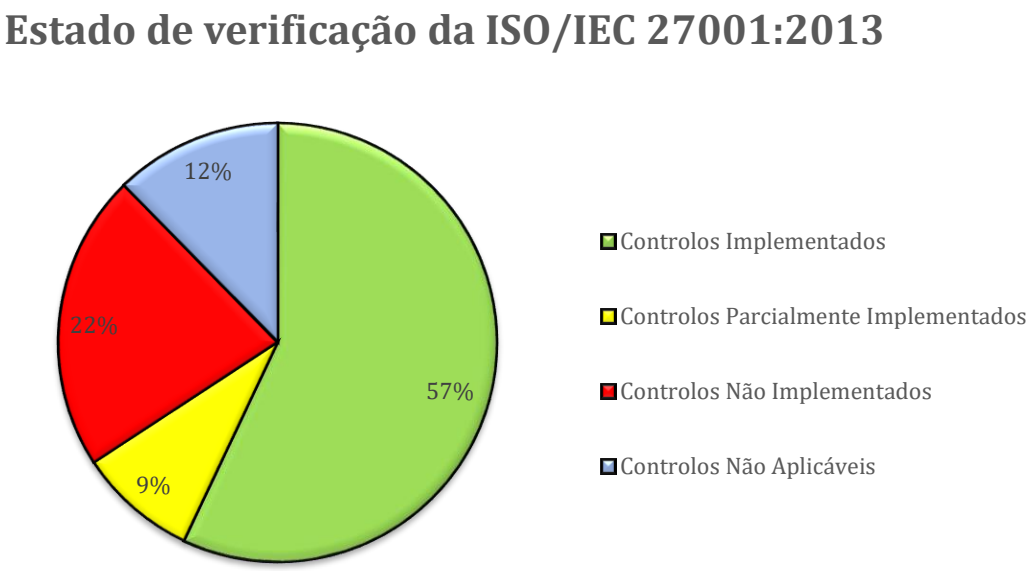


Figura 16 - Estado de Verificação dos Controlos Totais

Fonte: Elaboração própria

De acordo com o estado de verificação, analisou-se ao todo 114 controlos, sendo 65 os controlos definidos como implementados; 25 os controlos que não se encontravam implementados; 14 os controlos não aplicáveis à empresa, restando 10 controlos que parcialmente estão implementados.

Após a implementação da norma ISO/IEC 27001, e apesar de haver bastantes melhorias, existem controlos que se evidenciaram de modo significativo (figura 17).

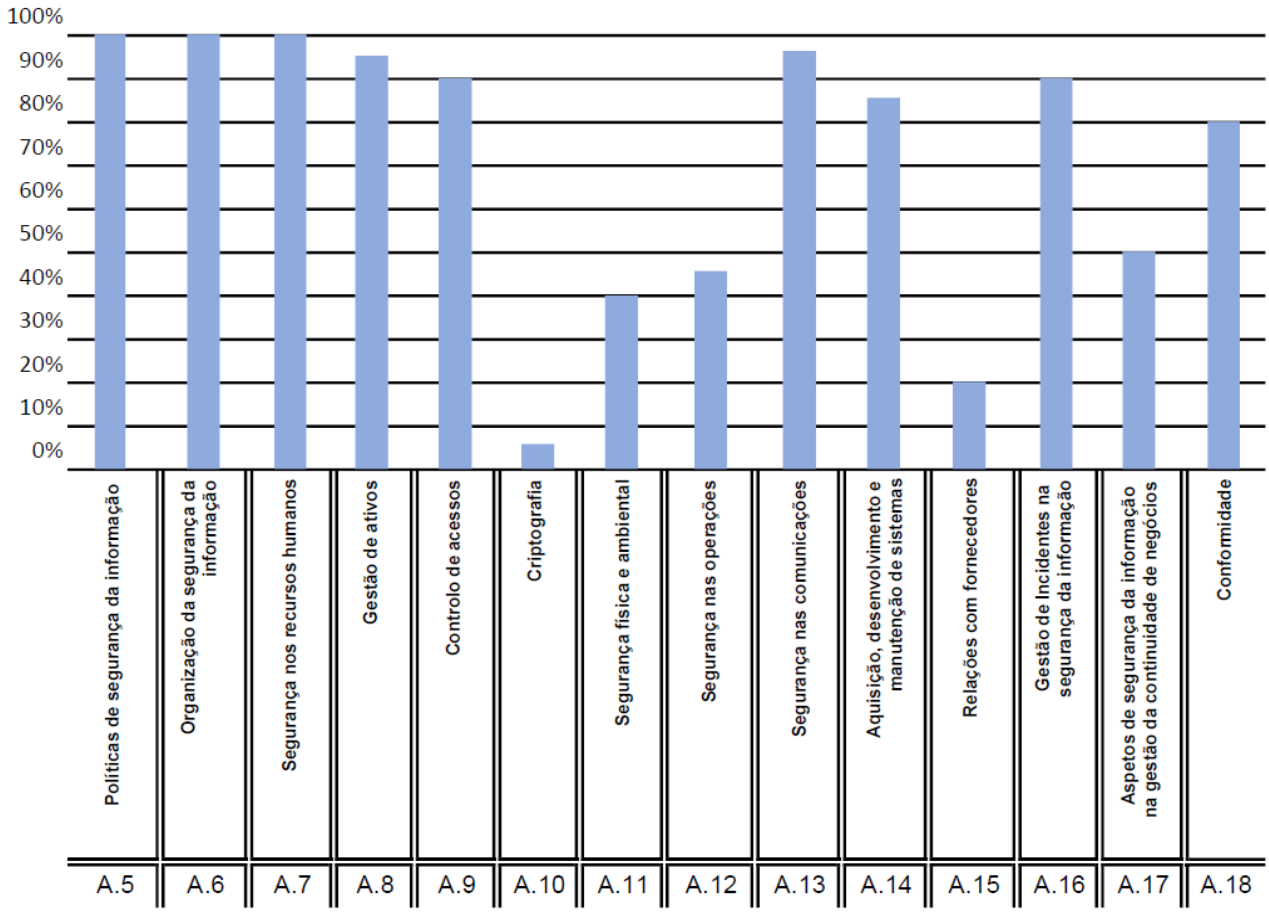


Figura 17 - Resultados por secção da auditoria da norma ISO/IEC 27001

Fonte: Elaboração própria

Face aos resultados apresentados da lista de verificação da auditoria, enumerou-se um conjunto de propostas de melhoria, nomeadamente:

1. Dada a ausência física do administrador e com a ambição de ser uma empresa reconhecida:
   - Recomenda-se a génese de um modelo do sistema de segurança da informação, capaz de compreender todas as políticas, princípios, procedimentos e outros elementos de orientação, com base em documentos legais e normativos existentes no âmbito da segurança da informação.
2. No contexto da análise e gestão de riscos da segurança da informação:
   - Recomenda-se a inserção da prática, capaz de definir e manter cenários de risco da

segurança da informação. Esta prática permite que a organização se antecipe, não atualmente dos riscos que não se deparam, mas daqueles que tardiamente poderão vir a desvendar na empresa.

3. No sentido de poder prever e antecipar possíveis falhas ou "não conformidades" das medidas e métricas já estabelecidas:
   - Recomenda-se a realização de avaliações e verificações regulares de conformidade. Deste modo, evita-se o hábito de só intervir quando uma ocorrência se torna não conformável. O mesmo deve-se aplicar aos controlos de segurança da informação definidos e implementados pela empresa.

4. Recomenda-se ao Departamento Financeiro, adotar uma política de transparência, que está diretamente ligada à organização e à divulgação clara e detalhada das contas.
   - Essa política é necessária para aumentar a confiança dos investidores.

5. Como é observável, nem todas as políticas e controlos se encontram registados e respetivamente associados aos riscos que se pretendem diminuir:
   - Recomenda-se a identificação e o registo de todos os controlos existentes e incluir os mesmos no tratamento e plano de risco de segurança da informação.
   - As políticas definidas nos diversos anexos devem ser elaboradas e atualizadas em intervalos regulares ou sempre que há atualizações nas mesmas;

6. Relativo ao controlo dos ativos existentes, tendo em conta que não é da direta responsabilidade do Departamento *Security*:
   - De extrema importância, recomenda-se a prática verificada regularmente, com o estabelecimento de controlos associados ao ciclo de vida do *software* para aplicações autodesenvolvidas e personalizadas.

7. No enquadramento da relação que a empresa mantem com os fornecedores, verifica-se que não há grande comunicação entre os mesmos:
   - Recomenda-se que a organização tenha uma participação mais direta e ativa com os fornecedores para a possibilidade de gerir vulnerabilidades, pontos de entrada e

alcançar controlos da segurança da informação. Devem ser implementados e mantidos os contactos com as entidades fornecedoras, para preparar e prever qualquer mudança futura;

8. Relativamente à identificação de identidades:
   - Verificou-se que apesar da organização verificar o histórico de antecedentes para os indivíduos que trabalham e entram na instalação, nomeadamente em áreas sensíveis, não se efetua uma prática segura com os visitantes. Recomenda-se adoção da prática presente;

9. Relativamente ao Departamento de Recursos Humanos empregue na organização:
   - É fulcral que estes tenham noções especificas e claras das suas funções e responsabilidades operacionais. Desta forma, e uma vez que não foi possível observar a sua existência, recomenda-se que a empresa defina com clareza todas as responsabilidades, tarefas e obrigações relativas à segurança da informação, igualmente a outras estruturas hierárquicas;

10. Todos os colaboradores da empresa com acesso a informações consideradas sensíveis, devem capacitar-se das suas responsabilidades, assim como um consentimento por escrito de confidencialidade;

11. A organização deve sensibilizar os colaboradores de que credenciais de autenticação são intransmissíveis e de caracter pessoal;

12. Durante os processos de desenvolvimento devem ser realizados testes padronizados regulares de segurança;

13. As prestações de serviços por parte dos trabalhadores devem ser identificadas, definidos em políticas as áreas e responsabilidades que atuam, realizando uma revisão dos direitos de acesso permitidos na empresa;

14. Todos os colaboradores que utilizam serviços e sistemas de informação na empresa, devem ser incentivados a relatar qualquer observação de falhas de segurança de informações ou qualquer tentativa suspeita.

Porém, nem tudo o que foi recomendado na empresa são associadas a melhorias ou particularidades que não estejam em implantadas. Sendo uma área a cada dia mais competitiva e severa, há um todo de vantagens que se estende sobre a concorrência, sendo fatores estes imprescindíveis para o sucesso de uma empresa.

A prestação de um serviço de qualidade é um dos principais requisitos para dar satisfação e confiança a um cliente, e para isso, é necessário a formação de uma equipa com capacidades e conhecimentos para solucionar ideias aos clientes.

5.8. Elaboração de um manual de boas práticas

Hoje em dia, é uma tarefa árdua fazer com que as empresas funcionem sem um adequado equipamento informático, recursos predominantes à organização ou sem uma organização que incute o bem-estar e segurança dos trabalhadores.

De facto, uma organização pode eventualmente ter prejuízos incalculáveis, ou, num caso mais grave, ser descontinuada por incidentes de segurança da informação envolvendo informações de nível confidencial.

Ao longo desta dissertação, referiu-se que não existe 100% de utilização adequada de segurança em qualquer empresa. É necessário rematar o que poderá ser uma porta aberta para intrusos e possíveis ataques que causem grandes prejuízos às organizações. É nesse intuito, imprescindível, envolver o ambiente da empresa com medidas que garantam a sua segurança efetiva, e claro, sempre que possível, a um custo justo e aceitável.

A determinação e a gestão de riscos são noções importantes na lei de proteção de dados e a dissertação vem ao encontro de uma necessidade criada pelo artigo 25.º do regulamento geral da proteção de dados, na qual fundamenta dois princípios que as empresas são obrigadas a cumprir (proteção de dados desde a conceção e por defeito), e tal como a empresa não adquire essa concretização, será necessário a elaboração de um manual de boas práticas.

Através do estudo das tabelas de verificação do estado dos controlos da ISO/IEC 27001, foram realizadas observações do funcionamento da empresa (anexo 4), para posteriormente implantação de recomendações no manual de boas práticas, com finalidade a colmatar eventuais erros, fraudes e sabotagens, aumentando a segurança e a qualidade dos funcionários, assim como o bom funcionamento da empresa Interaction Layer (encontra-se anexado na página 181).

6. Conclusões e perspetivas de desenvolvimento

Primeiramente, quero registar que a realização deste trabalho em ambiente empresarial, proporcionou-me uma experiência enriquecedora na envolvência com várias entidades sobre o tema da segurança da informação e temas afins como a gestão de riscos, bem como o conhecimento adquirido sobre a gestão de uma empresa, assentes na infraestrutura dos sistemas e tecnologias de informação da Interaction Layer.

Nesse sentido, estou convicta que a partilha de conhecimento entre os vários intervenientes que fizeram de alguma forma parte deste trabalho, resultou no geral uma experiência enriquecedora.

Dada a perspetiva, a realização deste presente trabalho e a análise de resultados obtidos, permitiu acumular vantagens relevantes para a definição do rumo a avaliar a norma ISO 27001 (associando diversas outras normas) e elaborar um manual de boas práticas. Por outro lado, teve algumas limitações de ordem técnica por não ser possível realizar testes de algumas das aplicações, sendo resolvido sem detalhe profundo nas entrevistas com os responsáveis da empresa. Impossibilitou o uso de ferramentas especializadas e, deste modo, impediu definir com maior rigor as recomendações e medidas que possam analisar e validar a arquitetura organizacional.

A realização de uma abordagem mais comprometida com a conformidade entre o regulamento e a ISO 27001, nomeadamente a nível de sistemas e serviços, poderá promover mudanças reais na maneira como os dados pessoais são tratados e como a privacidade dos utilizadores é protegida.

Como ponderação decorrente a trabalho futuro, perspetivam-se desafiantes tarefas que irão surgir assim que a empresa fizer a mudança de cede e provavelmente uma mudança em torno das condições e regras a que estes possam estar expostos, para além da interação transversal que haverá com as unidades orgânicas na concretização das diversas medidas propostas.

Eventualmente, a segurança da informação, para além de ter uma componente técnica e infraestrutural nas tecnologias de informação, tem sobretudo uma componente humana e processual no interior da empresa. Abranger, desde início, as pessoas que fazem parte dos processos organizacionais sobre temas relacionados com a segurança de informação e refletir a aplicabilidade de boas práticas é, sem sombra de dúvida, uma mais-valia no desenvolvimento do nosso trabalho pois, é através desta "experiência" de contacto com docentes já interiorizados com o tema, refletiu uma obtenção de aprendizagem e partilha de conhecimento

enorme.

A exploração desta área organizacional abre portas para a verdadeira atualização da gestão administrativa e criação de valor público com intervenientes das Tecnologias de informação e comunicação.

Torna-se iminente atualmente, a existência de um real conhecimento de todos os colaboradores no decorrer de todos os processos organizacionais, e só assim deverá ser possível a antecipação de falhas, e assegurar o serviço.

7. Referências bibliográficas

Amaral, Érico Hoff do, Marisa M. Amaral, and Raul C. Nunes. 2010. "Metodologia Para Cálculo Do Risco Por Composição de Métodos." In *X Simpósio Brasileiro Em Segurança Da Informação e de Sistemas Computacionais*, 461–73. Santa Maria, Brasil.

Bartens, Yannick, Steven Haes, Linda Eggert, Leonard Heilig, Kim Maes, Frederik Schulte, and Stefan Bob. 2014. "A Visualization Approach for Reducing the Perceived Complexity of COBIT 5." In *International Conference on Design Science Research in Information Systems*, edited by M.C. Tremblay, LNCS 8463:403–7. Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-319-06701-8_34.

Batalha, Jorge Martinez. 2017. "Novos Desafios Sobre a Proteção de Dados." *ResPublica*, no. 16: 201–17. http://hdl.handle.net/10437/8522.

Bertino, Elisa. 2016. "Data Security and Privacy: Concepts, Approaches, and Research Directions." In *2016 IEEE 40th Annual Computer Software and Applications Conference Data*, 1:400–407. https://doi.org/10.1109/COMPSAC.2016.89.

Boardman, Ruth, James Mullock, and Ariane Mole. 2019. "Guide to the General Data Protection Regulation (GDPR)." *Bird&Bird*, no. May. https://doi.org/10.1111/j.1751-1097.1994.tb09662.x.

Braga, Ascenção. 2000. "A Gestão Da Informação." *Millenium* 19: 1–10. http://repositorio.ipv.pt/handle/10400.19/903.

Carvalho, Ana Cristina de Melo, and Luís Filipe Coelho Antunes. 2018. "Metrics for Risk Assessment in Data Protection Impact Assessments." Faculdade de Ciências da Universidade do Porto. https://hdl.handle.net/10216/116275.

Charlet, Laurent. 2017. "ISO - The ISO Survey." ISO. 2017. https://www.iso.org/the-iso-survey.html.

Chopra, Kriti, Kunal Gupta, and Annu Lambora. 2019. "Future Internet: The Internet of Things-A Literature Review." *Proceedings of the International Conference on Machine Learning, Big Data, Cloud and Parallel Computing: Trends, Prespectives and Prospects, COMITCon 2019*, 135–39.

https://doi.org/10.1109/COMITCon.2019.8862269.

Clements, Tim, and Sue Milton. 2018. “Maintaining Data Protection and Privacy Beyond GDPR Implementation.” *ISACA*, 1–20.

Conselho Europeu para a Proteção de Dados. 2019. “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.” In , 1–27. Andrea Jelinek.

Correia, Carlos Manuel Rosa, and Vitor Manuel Pereira Duarte dos Santos. 2016. “Plano de Implementação Da Norma ISO/IEC 27001 No INEM.” Universidade Nova de Lisboa.

Cruz, José Manuel de Magalhães. 2012. “Segurança Da Informação: A Norma ISO/IEC 27000 e ISO/IEC 27001.” Porto.

Cuesta, Paco Fernández. 2018. “La Excepción a La Norma - Los Archivos En El Nuevo Regulamento General de Protección de Datos,” 29–31.

Dey, Manik. 2007. “Information Security Management - A Practical Approach.” *IEEE Xplore*, 1–6. https://doi.org/10.1109/AFRCON.2007.4401528.

Diamantopoulou, Vasiliki, Aggeliki Tsohou, and Maria Karyda. 2019. “From ISO / IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance,” 1–19.

Disterer, Georg. 2013. “ISO/IEC 27000, 27001 and 27002 for Information Security Management.” *Journal of Information Security* 4: 92–100. https://doi.org/http://dx.doi.org/10.4236/jis.2013.42011.

Faria, Cláudia Maria Félix Leite de, Maria Manuela Pinto, and Luís Antunes. 2018. “Gestão Da Cibersegurança Em Empresas Transnacionais Relacionadas Com Transações Financeiras Críticas de Espectro Macroeconómico.” Faculdade de Ciências da Universidade do Porto.

Fazendeiro, Ana. 2018. *Regulamento Geral Sobre a Proteção de Dados*. Edited by Almedina. 3ª Edição.

Feather, John, and Paul Sturges. 2003. *International Encyclopedia of Information and Library Science*. Edited by John Feather and Paul Sturges. *British Library Cataloguing in Publication Data*. Second Edi. http://repositorio.ipv.pt/handle/10400.19/903.

Ferreira, Sergio da Costa. 2017. *Sistemas de Informação Em Segurança*. Londrina.

Finck, Michèle, and Frank Pallas. 2019. "They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR." *SSRN Electronic Journal* 10 (1): 11–36. https://doi.org/10.2139/ssrn.3462948.

Fonseca, Alexandra, Alexandra Lourenço, Hélio Balinha, José Martins, José Dinis, and Liliana Marques. 2018. "O RGPD : A Articulação Entre a Gestão Da Informação e a Gestão Da Segurança Da Informação." *Cadernos de Biblioteconomia, Arquivística e Documentação*, 1–16.

Funk, Gerhard, Julia Hermann, Angelika Holl, Nikolay Jeliazkov, and Oliver Knörle. 2016. *Implementation Guideline ISO/IEC 27001:2013 - Practical Guideline for Implementing an ISMS in Accordance with the International Standard ISO/IEC 27001:2013*. *Isaca*. Berlin, Germany: ISACA Germany Chapter e.V. https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf.

Gonzales, Diego. 2018. "Diseño de Un Plan Estratégico de Seguridad de La Información, Mediante La Aplicación de Análisis de Riesgos Con La Norma ISO/IEC 27005 Caso de Estudio INAMHI." *INNOVA Research Journal*, 2018. https://doi.org/10.33890/innova.v3.n2.1.2018.672.

Hildebrandt, Mireille, and Laura Tielemans. 2013. "Data Protection by Design and Technology Neutral Law." *Computer Law and Security Review* 29 (5): 509–21. https://doi.org/10.1016/j.clsr.2013.07.004.

Hughes, J. Trevor, and Barday Kabir. 2018. "Bridging ISO 27001 to GDPR." *IAPP-One Trust Privacy Management Software*, 2018. https://iapp.org/media/pdf/resource_center/IAPP-OneTrust-Bridging-ISO-GDPR-final.pdf.

Interaction Layer. 2020. "Interaction Layer - Sobre a Empresa." Sobre a Empresa. 2020. https://interactionlayer.com/about-us.html.

International Organization for Standardization. 2019. "The ISO Survey of Management System Standard Certifications." https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0._Explanatory_note_on_ISO_Survey_2018_results.pdf?nodeid=20719021&vernum=-2.

———. 2020. “35.030 - IT Security.” Standards Catalogue. 2020. https://www.iso.org/ics/35.030/x/.

Li, He, Lu Yu, and Wu He. 2019. “The Impact of GDPR on Global Technology Development.” *Journal of Global Information Technology Management* 22 (1): 1–6. https://doi.org/10.1080/1097198X.2019.1569186.

Lopes, Isabel Maria, Teresa Guarda, and Pedro Oliveira. 2019. “How ISO 27001 Can Help Achieve GDPR Compliance.” *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, no. June: 1–6. https://doi.org/10.23919/cisti.2019.8760937.

Lunardi, Guilherme, Pietro Cunha Dolci, and Antonio Carlos Gastaud Maçada. 2010. “Adoção de Tecnologia de Informação e Seu Impacto No Desempenho Organizacional: Um Estudo Realizado Com Micro e Pequenas Empresas.” *Revista de Administração*, 2010. https://doi.org/10.1016/s0080-2107(16)30505-2.

Magalhães, Filipa Matias, and Maria Leitão Pereira. 2018. *Regulamento Geral de Proteção de Dados - Manual Prático*. Edited by Vida Económica. 2ª Edição. Porto.

Maingak, Akmal Zaifullah, Candiwan, and Listyo Dwi Harsono. 2018. “Information Security Assessment Using ISO/IEC 27001:2013 Standard on Government Institution.” *Trikonomika* 17 (1): 28–37. https://doi.org/10.23969/trikonomika.v17i1.1138.

Mamede, Henrique São. 2015. “Notas Leitura/Recensão Crítica Proteção Dados Pessoais.” *Revista de Ciências Da Computação Nº10*, 2015. http://ec.europa.eu/justice/data-protection/.

Milicevic, Danijel, and Matthias Goeken. 2010. “Ontology-Based Evaluation of ISO 27001.” *IFIP Advances in Information and Communication Technology*, 93–102. https://doi.org/10.1007/978-3-642-16283-1_13.

Moreira, Tiago Filipe Monteiro. 2018. “O Impacto Do Regulamento Geral de Proteção de Dados Nas Organizações: Um Novo Paradigma.” Instituto Superior de Contabilidade e Administração de Coimbra.

Nakamura, Emílio Tissato. 2016. *Segurança Da Informação e de Redes*. Edited by Londrina. Avenida Paris.

Nasser, Adel. 2017. “Information Security Gap Analysis Based on ISO 27001: 2013 Standard:

A Case Study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen A." *International Journal of Scientific Research in Multidisciplinary Studies* 3 (11): 4–13. https://doi.org/10.26438/ijsrms/v3i11.413.

NP ISO/IEC 27001. 2013. *Information Technology - Security Techniques - Information Security Management Systems - Requirements*. Edited by SNV Schweizerische Normen-Vereinigung. 2nd ed. ISO. https://doi.org/10.1109/IEEESTD.2005.339589.

NP ISO/IEC 27005. 2008. *Information Technology -Security Techniques -Information Security Risk Management*. 1st ed. http://www.iso.org.

NP ISO/IEC 31000. 2018. *Risk Management - Guidelines*. 2nd ed.

Nurse, Jason R. C., Sadie Creese, and David De Roure. 2017. "Security Risk Assessment in Internet of Things Systems." *IT Professional*, 2017.

Oliveira, Ricardo André Pereira, and Ana Luísa do Carmo Correia Respício. 2015. "Análise de Risco Associado a Quebras de Serviço." Faculdade de Ciências da Universidade de Lisboa.

Oliveira, Thiago Rodrigues. 2017. "Implantação de Políticas de Segurança Da Informação Em Uma Pequena Empresa." *Revista Eletrónica de Sistemas de Informação e de Gestão Tecnológica*, 2017.

Peciña, Koldo, Alfonso Bilbao, and Enrique Bilbao. 2011. "Physical and Logical Security Risk Analysis Model." *Proceedings - International Carnahan Conference on Security Technology*, 1–7. https://doi.org/10.1109/CCST.2011.6095895.

Pimenta, Alexandre, and Rui Filipe Quaresma. 2016. "A Segurança Dos Sistemas de Informação e o Comportamento Dos Usuários." *Journal of Information Systems and Technology Management* 13 (3): 533–52. https://doi.org/10.4301/s1807-17752016000300010.

Pinheiro, Alexandre Sousa, Cristina Pimenta Coelho, Tatiana Duarte, Carlos Jorge Gonçalves, and Catarina Pina Gonçalves. 2018. *Comentário Ao Regulamento Geral de Proteção de Dados*. Edited by Almedina. Coimbra.

Pinho, Frederico António Sá Oliveira, Manuel Correia, and Luís Antunes. 2017. "Anonimização de Bases de Dados Empresariais de Acordo Com a Nova

Regulamentação Europeia de Proteção de Dados." Faculdade de Ciências da Universidade do Porto. https://cracs.fc.up.pt/sites/default/files/MSI_Dissertacao_FINAL.pdf.

Prashar, Anupama. 2017. "Adopting PDCA (Plan-Do-Check-Act) Cycle for Energy Optimization in Energy-Intensive SMEs." *Journal of Cleaner Production* 145: 277–93. https://doi.org/10.1016/j.jclepro.2017.01.068.

Ramos, Alexandra Lemos. 2016. "O Princípio Da Administração Aberta versus O Princípio Da Proteção Dos Dados Pessoais." Facldade de Direito da Universidade de Lisboa.

Sêmola, Marcos. 2014. "Sociedade Do Conhecimento." In *Gestão Da Segurança Da Informação - Uma Visão Executiva*, edited by Elsevier, 2ª Edição, 1–22. São Paulo, Brasil.

Shivashankarappa, Arun, Leonid Smalov, Ramalingam Dharmalingam, and N. Anbazhagan. 2012. "Implementing It Governance Using Cobit: A Case Study Focusing on Critical Success Factors." In *World Congress on Internet Security, WorldCIS-2012*, 144–49. IEEE.

Shojaie, Bahareh, Hannes Federrath, and Iman Saberi. 2014. "Evaluating the Effectiveness of ISO 27001:2013 Based on Annex A." In *9th International Workshop on Frontiers in Availability, Reliability and Security, FARES 2014*, 1–6. Swizerland: IEEE. https://doi.org/10.1109/ARES.2014.41.

———. 2015. "The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001." In *10th International Conference on Availability, Reliability and Security*, 159–67. IEEE. https://doi.org/10.1109/ARES.2015.25.

Sousa, Mariana Leite, Olívia Manuela Marques Pestana, and Ricardo Cruz Correia. 2017. "OpenEHR Como Solução Para o Regulamento Geral de Proteção de Dados Na Área Da Saúde." Faculdade de Engenharia da Universidade do Porto. https://www.bad.pt/eventos/wp-content/uploads/2018/01/CIGIA_COM_10.pdf.

Stallings, William. 2015. *Criptografia e Segurança de Redes - Princípios e Práticas*. 6ª Edição. São Paulo, Brasil: Pearson Education.

Veale, Michael, Reuben Binns, and Jef Ausloos. 2018. "When Data Protection by Design and Data Subject Rights Clash." *International Data Privacy Law* 8 (2): 105–23.

https://doi.org/10.1093/idpl/ipy002.

Velasco, Joffre, Rodrigo Ullauri, Luis Pilicita, Bolivar Jacome, Pablo Saa, and Oswaldo Moscoso-Zea. 2018. “Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry.” In *3rd International Conference on Information Systems and Computer Science, INCISCOS*, 294–300. Quito, Ecuador: IEEE. https://doi.org/10.1109/INCISCOS.2018.00049.

Weber, Rolf H. 2010. “Internet of Things - New Security and Privacy Challenges.” *Computer Law and Security Review* 26 (1): 23–30. https://doi.org/10.1016/j.clsr.2009.11.008.

Whitman, Michael E, and Herbert J Mattord. 2018. *Principles of Information Security*. *Cengage Learning*. Sixth Edit. Boston, USA.

Yamamoto, Ryuichi. 2016. “Large-Scale Health Information Database and Privacy Protection.” In *Japan Medical Association Journal*, 59:91–109.

Zúquete, André. 2008. *Segurança Em Redes Informáticas*. Edited by FCA - Editora de Informática. 2ª edição. Lisboa. https://catalogo.up.pt/F/?func=find-b&request=Segurança+em+Redes+Informáticas&find_code=WRD&x=0&y=0&filter_code_1=WLN&filter_request_1=&filter_code_2=WCN&filter_request_2=&filter_code_3=WYR&filter_request_3=&filter_code_5=WFMT&filter_request_5=&.

Anexos

Anexo 1 – Mapeamento norma ISO/IEC 27001 e RGPD

NORMA ISO/IEC 27001:2013		REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (RGPD)		
CONTROLO	**RESUMO**	**N.º**	**ARTIGO**	**REQUISITO**
CAPÍTULO I - DISPOSIÇÕES GERAIS				
A. 18.1.4	O RGPD diz respeito à proteção e livre circulação de "dados pessoais", que define ser "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;" (cf. artigo 4.º, do RGPD).	1.º	Objeto e objetivos	A ISO 27001 diz respeito aos riscos da informação, integrando a gestão de controlos de segurança da informação e riscos inaceitáveis ás informações das organizações. No RGPD, a privacidade é em grande parte uma questão de proteger as informações pessoais, particularmente dados confidenciais. A norma menciona obrigações de conformidade relacionadas com a privacidade e proteção de informações pessoais.
A.5 – A.18	A ISO 27001 diz respeito a informações em geral, não apenas a dados, sistemas, aplicativos e redes de computadores. É uma estrutura ampla, construída em torno de um sistema de gestão. A ISO 27001 trata os riscos e controlos de informação em toda a	2.º	Âmbito de aplicação material	O RGPD refere-se ao "tartamento de dados pessoais total ou parcialmente por meios automatizados ..." (ex. sistemas, aplicativos e redes de computadores), num contexto comercial ou organizacional.

	organização, indo além da privacidade e conformidade.			
A. 18	Uma organização que interaja com pessoas na União Europeia pode-se enquadrar no RGPD, principalmente se recolher informações pessoais.	3.º	Âmbito de aplicação territorial	O RGPD diz respeito essencialmente a dados pessoais de pessoas na União Europeia, sejam eles processados na UE ou em outro local.
Exigência 3	A ISO/IEC 27000 define a maioria dos termos da ISO 27001, incluindo alguns termos de privacidade. Além de verificar se as definições corporativas não entram em conflito com o RGPD.	4.º	Definições	Os termos relacionados com a privacidade do RGPD são aqui formalmente definidos.
CAPÍTULO II - PRINCÍPIOS				
6.1.2; A.8.1.1; A.8.2; A.8.3; A.9.1.1; A.9.4.1; A.10; A.13.2; A.14.1.1; A.15; A.17; A.18	Os processos de negócios devem proteger as informações pessoais, exigindo um conjunto de controlos tecnológicos e processuais. (cf. artigo 25.º, do RGPD). Para atender a esses requisitos, as organizações precisam de saber onde estão alocadas as informações pessoais, classificá-las e aplicar medidas apropriadas.	5.º	Princípios relativos ao tratamento de dados pessoais	Os dados pessoais devem ser: (a) processados de forma legal, justa e transparente; (b) recolhidos apenas para fins especificados; (c) adequados, relevantes e limitados; (d) precisos; (e) mantidos não mais do que o necessário; (f) processados com segurança para garantir sua integridade e confidencialidade.
6.1.2; A.14.1.1; A.18.1.1	Deve ser abrangido na avaliação e tratamento dos riscos da informação. Estes são requisitos de negócios para limitar e proteger informações pessoais. Muitos controlos de segurança são necessários para abrandar riscos inaceitáveis de	6.º	Licitude do tratamento	O tratamento legal deve ser: (a) consentido pelo sujeito para a finalidade declarada; (b) ser exigido por um contratante; (c) necessário para proteger os interesses vitais de alguém; (d) exigido para interesse público ou

	informações que não podem ser evitadas (a não recolha) ou compartilhadas (confiança).			uma autoridade oficial; (e) ser limitado se o sujeito for criança.
A.8.2.3; A.12.1.1; A.13.2.4; A.18.1.3; 6.1.2; A.14.1.1; A.8.3.2; A.13.2	Necessário um requisito para solicitar o consentimento informado para o tratamento. E ser capaz de demonstrar isso, além de que os procedimentos precisam estar em vigor.	7.º	Condições aplicáveis ao consentimento	O consentimento do titular dos dados deve ser de livre vontade retirado facilmente a qualquer momento.
	Aplicam-se principalmente no momento em que as informações são recolhidas (ex. obter o consentimento dos pais).	8.º	Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação	Restrições especiais aplicam-se ao consentimento das crianças.
A.8.2.1; A.8.2.3; A.14.1.1	É importante identificar onde os dados confidenciais podem ser processados e se é necessário obter o consentimento (cf. artigo 7.º, do RGPD).	9.º	Tratamento de categorias especiais de dados pessoais	Restrições especiais aplicam-se a dados particularmente sensíveis relativos a opiniões políticas e biometrias de uma pessoa. O tratamento dessas informações é proibido por padrão, a menos que seja dado consentimento.
A.7.1; A.8.2.1; A.8.2.3; 6.1.2; A.14.1.1; A.7.1	O uso dessas informações deve ser identificado e processado apenas em circunstâncias específicas, necessárias para a verificação de antecedentes e perfis de risco de fraude.	10.º	Tratamento de dados pessoais relacionados com condenações penais e infrações	Restrições também se aplicam a dados pessoais relativos a condenações e infrações penais.
A.8.2.1; A.8.2.3; 6.1.2; A.14.1.1	Evitar riscos à informação é uma boa opção.	11.º	Tratamento que não exige identificação	Restrições não se aplicam se a pessoa não puder ser identificada a partir dos dados mantidos.
CAPÍTULO III - DIREITOS DO TITULAR DOS DADOS				

Secção 1 - Transparência e regras para o exercício dos direitos dos titulares dos dados				
A.12.1.1; A.14.1.1; A.16	Afeta a redação de formulários web, notificações e scripts, além dos processos. Relevante para a gestão de incidentes, responder e manter registos dessas comunicações (ex. limitar ou cobrar por solicitações excessivas).	12.º	Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados	As comunicações com os titulares dos dados devem ser transparentes, claras e facilmente compreendidas.
Secção 2 - Informação e acesso aos dados pessoais				
A.8.2; A.8.2.3; A.12.1.1; A.14.1.1; A.16	Os procedimentos para o fornecimento de informações sobre o "controlador de dados" e das finalidades para o tratamento dos dados precisam de ser definidos e implementados.	13.º	Informações a facultar quando os dados pessoais são recolhidos junto do titular	Quando os dados pessoais são recolhidos, as pessoas devem receber vários itens específicos de informações, como detalhes do "controlador de dados" e "responsável pela proteção de dados", se as suas informações serão exportadas (especialmente fora da UE) e por quanto tempo as informações serão mantidas.
A.8.2.1; A.8.2.3; A.12.1.1; A.14.1; A.16	(Ver artigo 13.º).	14.º	Informações a facultar quando os dados pessoais não são recolhidos junto do titular	Notificação são idênticas ao artigo 13.º. Aplicam-se se as informações pessoais forem obtidas indiretamente (ex. lista externa), caso seja, devem ser informadas dentro de um mês.
A.8.1.1; A.8.2.1; A.12.1.1; A.13.2.1; A.14.1.1	Os direitos do titular, incluem a capacidade de obter cópias das suas informações, divulgando a natureza do tratamento e informações sobre os controlos se os seus dados forem exportados.	15.º	Direito de acesso do titular dos dados	As pessoas têm o direito de descobrir se a organização possui as suas informações pessoais e para que efeito elas estão sendo usadas e divulgadas. Contudo, as pessoas também têm o direito de obter uma cópia das suas informações pessoais.
Secção 3 - Retificação e apagamento				

A.12.1.1; A.14.1; A.9; A.16; A.12.3; A.18.1.3	Implica requisitos funcionais para verificar e editar as informações armazenadas, com controlos associados à identificação, autenticação, acesso e validação.	16.º	Direito de retificação	As pessoas têm o direito de corrigir, completar e esclarecer as suas informações pessoais.
6.1.2; A.14.1.1; A.9; A.16; A.12.3; A.8.3.2	Forma de retirar o consentimento (cf. artigo 7.º, do RGPD). Implica requisitos funcionais do sistema para poder apagar informações armazenadas específicas (ex. autenticação, acesso e validação).	17.º	Direito ao apagamento dos dados («direito a ser esquecido»)	As pessoas têm o direito de serem esquecidas (as suas informações pessoais serem apagadas).
6.1.2; A.8.2.1; A.8.2.3; A.12.1.1; A.14.1.1; A.16; A.12.3; A.18.1.1	Há maneiras de identificar os dados específicos que devem ser restritos. Pode afetar as cópias de backup e arquivos digitais (cf. artigo 7.º e 12.º, do RGPD).	18.º	Direito à limitação do tratamento	As pessoas têm o direito de restringir o tratamento das suas informações pessoais.
A.12.1.1; 6.1.2; A.14.1.1; A.16	Informar e atualizar o remetente é uma parte pactual do processo da gestão de incidentes, havendo processos de reclamações de privacidade ou solicitações.	19.º	Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento	As pessoas têm o direito de saber o resultado das solicitações das suas informações pessoais, caso sejam corrigidas, concluídas, apagadas ou restritas.
6.1.2; A.13; A.14.1.1; A.8.3; A.10; A.18.1.3	Dados extraídos devem ser limitados às pessoas identificadas e autenticadas, e devem ser comunicados com segurança, provavelmente criptografados (cf. artigo 9.º, do RGPD).	20.º	Direito de portabilidade dos dados	As pessoas têm o direito de obter uma cópia eletrónica "portátil" utilizável de seus dados pessoais.

	Porém, podem também implicar apagar ou restringir dados e confirmá-los (cf. artigo 17.º e 18.º, do RGPD).			
Secção 4 - Direito de oposição e decisões individuais automatizadas				
6.1.2; A.12.1.1; A.14.1.1; A.16; A.12.3	Há maneiras de identificar os dados específicos que não devem ser processados (cf. artigo 18.º, do RGPD).	21.º	Direito de oposição	As pessoas têm o direito de se opor quando as suas informações sejam usadas para fins de criação de perfil e marketing.
6.1.2; A.12.1.1; A.14.1.1; A.16	Os sistemas de criação de perfil que envolvam informações pessoais devem permitir revisões e substituições manuais, com os devidos controlos de autorização e acesso.	22.º	Decisões individuais automatizadas, incluindo definição de perfis	As pessoas têm o direito de solicitar que, as decisões do tratamento das suas informações pessoais sejam revistas.
Secção 5 - Limitações				
A.18.1.1	Preocupa principalmente as autoridades e os seus sistemas de negócio (ex. alfândega, imigração, forças de segurança). Porém também afeta organizações privadas (ex. setor jurídico, indústrias e serviços financeiros).	23.º	Limitações	As leis nacionais podem modificar ou substituir vários direitos/restrições para a segurança nacional.
CAPÍTULO IV - RESPONSÁVEL PELO TRATAMENTO E SUBCONTRATANTE				
Secção 1 – Obrigações gerais				
Exigência 4, 5, 6, 7, 8, 9, 10 + Anexo A	Controlos de privacidade devem ser implementados (políticas e procedimentos que tratem dos riscos de informações e das obrigações de conformidade).	24.º	Responsabilidade do responsável pelo tratamento	O "controlador", é responsável pela implementação de controlos de privacidade (políticas e códigos de conduta), considerandos no RGPD.

	Daí fazer sentido integrar e coordenar a privacidade com o ISMS com a norma ISO 27001 e a gestão de conformidade.			
Exigência 6 + Anexo A	Existem razões de negócio para investir na privacidade, incluindo riscos de informações e conformidade, bem como opções de implementação. Estas razões são uma boa maneira de garantir suporte e envolvimento da organização. Privacidade por conceção e por defeito são exemplos de princípios de privacidade implícitos à especificação, desenvolvimento e manutenção de sistemas e processos de TI relacionados com a privacidade.	25.º	Proteção de dados desde a conceção e por defeito	Tendo em conta os riscos, custos e benefícios, deve haver proteção para as informações pessoais por conceção e por defeito.
Exigência 5.3, 9.1 + A.13.2; A.15; A.16; A.18.1	Organizações devem gerir laços com parceiros de negócios, garantindo que a privacidade e a segurança das informações não falhem (ex. violações ou solicitações de acesso e manter um nível garantido de conformidade com o RGPD).	26.º	Responsáveis conjuntos pelo tratamento	Organizações são responsáveis por determinar e cumprir os requisitos de privacidade de forma colaborativa.
Exigência 5.3, 7.5.1 + A.15; A.18.1.4	O Diretor da Proteção de Dados, deve ser responsável por garantir que isso seja feito corretamente.	27.º	Representantes dos responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na União	As organizações fora da Europa devem nomear representantes da privacidade na Europa, se cumprirem determinadas condições (ex. fornecer bens e serviços para europeus).
Exigência 8.2, 9.1 + A.15;	Fornecedores de serviços podem ser questionados sobre o seu status de conformidade com RGPD, políticas de	28.º	Subcontratante	Caso uma organização use um ou mais subcontratantes para processar informações pessoais, devem garantir

A.18.1.1; A.18.1.3; A.18.1.4	privacidade e outros controlos, ter termos e responsabilidades de conformidade.			que eles também estejam em conformidade com o RGPD.
A.5 – A.18	Os subcontratantes precisam de proteger e controlar as informações pessoais da mesma maneira que os controladores.	29.º	Tratamento sob a autoridade do responsável pelo tratamento ou do subcontratante	Os subcontratantes devem processar apenas informações pessoais de acordo com as instruções do controlador e as leis aplicáveis.
Exigência 7.5	Através da informação documentada.	30.º	Registos das atividades de tratamento	Controladores devem manter a documentação referente à privacidade, como objetivos para os quais as informações pessoais são recolhidas e processadas.
A.6.1.3	Contatar com as autoridades.	31.º	Cooperação com a autoridade de controlo	Organizações devem cooperar com as autoridades.
Secção 2 – Segurança dos dados pessoais				
Exigência 8.2, 8.3 + Anexo A	O RGPD menciona exemplos de controlo, como criptografia, anonimização e recuperação, envolvendo aspetos de confidencialidade, integridade e disponibilidade dos dados. Um *ISMS* da ISO/IEC 27001 fornece uma estrutura coerente e estruturada para a gestão da privacidade, juntamente com outros riscos de informações e controlos.	32.º	Segurança do tratamento	Organizações devem implementar e manter medidas de segurança organizacional apropriadas para abordar riscos de informações.
A.16; A.18.1.4	As violações são tratadas como incidentes no SGSI, mas as obrigações específicas do RGPD, (prazo de três	33.º	Notificação de uma violação de dados pessoais à autoridade de controlo	Violações de privacidade que prejudiquem informações pessoais, devem ser notificadas imediatamente às

	dias para a notificação às autoridades) devem ser cumpridas.			autoridades (dentro de três dias após tomar conhecimento delas).
A.16; A.18.1.4	Obviamente existem questões relacionadas com a natureza da divulgação. Normalmente, isso faz parte do processo de gestão de incidentes, na qual, envolve a administração, especialistas e consultores. Evitar essa situação, custos e agravamento é um dos argumentos mais fortes para investir adequadamente em medidas preventivas.	34.º	Comunicação de uma violação de dados pessoais ao titular dos dados	Violações de privacidade que prejudiquem informações pessoais, devem ser notificadas imediatamente às pessoas afetadas.
Secção 3 – Avaliação de impacto sobre a proteção de dados e consulta prévia				
6.1.2; A.6.1.3; A.8.2.1	O RGPD sugere a integração da avaliação de riscos à privacidade como parte das atividades de rotina de avaliação dos riscos para projetos de negócios e novos desenvolvimentos de sistemas de TI.	35.º	Avaliação de impacto sobre a proteção de dados	Os impactos dos riscos de privacidade devem ser avaliados, quando estes são significativos. Situações que são significativamente arriscadas devem ser definidas pelas autoridades nacionais.
6.1.2; A.6.1.3; A.8.2.1	O RGPD é envolvido pelas políticas corporativas relacionadas com “altos” riscos à privacidade. Mas, contribuições das autoridades podem ser úteis nas decisões estratégicas.	36.º	Consulta prévia	Os riscos de privacidade avaliados como "altos" [indefinidos] devem ser notificados às autoridades, dando-lhes a chance de comentar.
Secção 4 – Encarregado da proteção de dados				
Exigência 5.3, + A.6.1.1; A.18.1.4	Além do que remete o RGPD, o papel do "Responsável pela privacidade" ou “Encarregado da proteção de dados”, é muito mais valioso, seja em que circunstância for. Assim, um ponto	37.º	Designação do encarregado da proteção de dados	O responsável pela proteção de dados, deve ser identificado sob circunstâncias especificadas (ex. órgãos públicos).

	focal corporativo designado para a privacidade faz sentido para praticamente todas as organizações.			
Exigência 5.3 + A.6.1.1; A.18.1.4	Sem o apoio e envolvimento da organização, um Diretor de Privacidade é inapto e ininteligível.	38.º	Posição do encarregado da proteção de dados	O responsável pela proteção de dados deve ser apoiado pela organização e envolvido nas questões de privacidade.
Exigência 5.3 + A.6.1.1; A.18.1.4	Requisitos do RGPD formam a base de uma do cargo de Responsável pela Privacidade.	39.º	Funções do encarregado da proteção de dados	O responsável pela proteção de dados deve oferecer consultoria nas questões de privacidade, conformidade, contactar autoridades e abordar riscos de privacidade.
Secção 5 – Códigos de conduta e certificação				
Exigência 5.3 + A.6.1.1; A.18.1.4	Ação vantajosa de acrescentar peso aos códigos do setor, necessariamente para cumprir um mandato legal e completo. Além disso, as normas ISO/IEC 27001 oferecem orientações de boas práticas.	40.º	Códigos de conduta	Autoridades, associações e órgãos da indústria elaboram códigos de conduta do RGPD e da privacidade, e quando formalmente aprovados, seguem para a implementação dos mecanismos de conformidade.
Exigência 5.3 + A.6.1.1; A.18.1.4	Ação vantajosa de acrescentar peso aos códigos do setor, necessariamente para cumprir um mandato legal e completo. Além disso, as normas ISO/IEC 27001 oferecem orientações de boas práticas.	41.º	Supervisão dos códigos de conduta aprovados	Os órgãos responsáveis pelos códigos de conduta são obrigados a controlar a conformidade, necessariamente sem prejuízo.
Exigência 5.3 + A.6.1.1; A.18.1.4	O RGPD dá em algum grau reconhecimento oficial.	42.º	Certificação	Esquemas de certificação da proteção de dados que ofereçam selos e marcas de conformidade, devem ser registados.
Exigência 5.3 + A.6.1.1; A.18.1.4	Com o intuito de melhorar a credibilidade e significado às autenticações e marcas de privacidade.	43.º	Organismos de certificação	Organismos de certificação que concedem autenticações e marcas de conformidade devem ser competentes e

				credenciados para esse fim. Porém a Comissão Europeia deve impor normas para os esquemas de certificação.
CAPÍTULO V - TRANSFERÊNCIAS DE DADOS PESSOAIS PARA PAÍSES TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS				
-	"Introdução" (Preâmbulo)	44.º	Princípio geral das transferências	Transferências internacionais e tratamento de informações pessoais devem atender aos requisitos estabelecidos nos artigos.
A.18.1.4	Formalidades devem ser tratadas pela Comissão Europeia. Envolvem evitar transferências para outros países, controlar as listas oficiais de alterações e garantir que os contratos e controlos de privacidade estejam em vigor (cf. artigo 28.º, do RGPD).	45.º	Transferências com base numa decisão de adequação	A transferência de dados para países na qual, acordos ou leis de privacidade não são considerados adequados pela Comissão Europeia, exigem garantias adicionais que sejam adequadas.
A.18.1.4	Uma organização deve implementar e garantir que os controlos de privacidade sejam adequados, antes de transferir dados pessoais para esses países (cláusulas contratuais e atividades de conformidade).	46.º	Transferências sujeitas a garantias adequadas	A transferência de dados para países na qual, acordos ou leis de privacidade não são considerados adequados pela Comissão Europeia, exigem garantias adicionais que sejam adequadas.
A.18.1.4	Poderão afetar tratados contratuais, acordos de conformidade e responsabilidades.	47.º	Regras vinculativas aplicáveis às empresas	Autoridades podem aprovar regras jurídicas de privacidade, que permitam transferências para países não aprovados.
A.18.1.4; A.16	Ocorrências tratadas por especialistas em conformidade legal e regulatória.	48.º	Transferências ou divulgações não autorizadas	Requisitos das organizações europeias de autoridades fora da Europa para divulgação não autorizada de dados

			pelo direito da União Europeia	pessoais podem ser inválidos, a menos que hajam acordos internacionais.
A.18.1.4	A Comissão Europeia está a tomar medidas cautelosas, visto que os riscos à privacidade são maiores.	49.º	Derrogações para situações específicas	Para países não aprovados, aplicam-se consentimentos explícitos aos titulares dos dados.
Não aplicável	Não aplicável	50.º	Cooperação internacional no domínio da proteção de dados pessoais	Cooperação das autoridades internacionais na privacidade dos dados.
CAPÍTULO VI - AUTORIDADES DE CONTROLO INDEPENDENTES				
Secção 1 – Estatuto independente				
Não aplicável	Não aplicável	51.º	Autoridade de controlo	Preocupação por parte dos órgãos nacionais que supervisionam a privacidade dos dados.
		52.º	Independência	
		53.º	Condições gerais aplicáveis aos membros da autoridade de controlo	
		54.º	Regras aplicáveis à constituição da autoridade de controlo	
Secção 2 – Competência, atribuições e poderes				
Não aplicável	Não aplicável	55.º	Competência	Preocupação por parte dos órgãos nacionais que supervisionam a privacidade dos dados.
		56.º	Competência da autoridade de controlo principal	
		57.º	Atribuições	

		58.º	Poderes	
		59.º	Relatórios de atividades	
CAPÍTULO VII - COOPERAÇÃO E COERÊNCIA				
Secção 1 – Cooperação				
Não aplicável	Não aplicável	60.º	Cooperação entre a autoridade de controlo principal e as outras autoridades de controlo interessadas	Relativo às autoridades responsáveis pela supervisão e pelo Conselho de Proteção de Dados da União Europeia.
		61.º	Assistência mútua	
		62.º	Operações conjuntas das autoridades de controlo	
Secção 2 – Coerência				
Não aplicável	Não aplicável	63.º	Procedimento de controlo da coerência	Relativo às autoridades responsáveis pela supervisão e pelo Conselho de Proteção de Dados da União Europeia.
		64.º	Parecer do Comité	
		65.º	Resolução de litígios pelo Comité	
		66.º	Procedimento de urgência	
		67.º	Troca de informações	
Secção 3 – Comité europeu para a proteção de dados				
Não aplicável	Não aplicável	68.º	Comité Europeu para a Proteção de Dados	

		69.º	Independência	Relativo às autoridades responsáveis pela supervisão e pelo Conselho de Proteção de Dados da União Europeia.
		70.º	Atribuições do Comité	
		71.º	Relatórios	
		72.º	Procedimento	
		73.º	Presidente	
		74.º	Funções do presidente	
		75.º	Secretariado	
		76.º	Confidencialidade	
CAPÍTULO VIII - VIAS DE RECURSO, RESPONSABILIDADE E SANÇÕES				
Não aplicável	Não aplicável	77.º	Direito de apresentar reclamação a uma autoridade de controlo	Autoridades de supervisão podem encarregar-se de reclamações de privacidade.
		78.º	Direito à ação judicial contra uma autoridade de controlo	
		79.º	Direito à ação judicial contra um responsável pelo tratamento ou um subcontratante	
		80.º	Representação dos titulares dos dados	
		81.º	Suspensão do processo	

A.18.1.4	Proteção de informação de caracter pessoal.	82.º	Direito de indemnização e responsabilidade	Uma pessoa prejudicada por violações do RGPD, tem direito a uma compensação do responsável de hierarquia superior.
Exigência 6 + A.18.1.4	Coimas administrativas impostas pelas autoridades de supervisão têm critérios, que, dependendo das circunstâncias, as mesmas podem chegar a 20 milhões de euros.	83.º	Condições gerais para a aplicação de coimas	Coimas são uma resistência significativa do impacto potencial de violações da privacidade.
Exigência 6 + A.18.1.4	Sanções podem ser impostas, devendo ser "eficazes e dissuasivas".	84.º	Sanções	Coimas são uma resistência significativa do impacto potencial de violações da privacidade.
CAPÍTULO IX - DISPOSIÇÕES RELATIVAS A SITUAÇÕES ESPECÍFICAS DE TRATAMENTO				
Exigência 6 + A.18.1.1; A.18.1.4	Existem riscos de informação a serem identificados, avaliados e tratados quando há vinculação de informações pessoais.	85.º	Tratamento e liberdade de expressão e de informação	Devem equilibrar direitos de privacidade e proteção de dados através de leis contra a liberdade de expressão, jornalismo e/ou pesquisas acadêmicas.
Exigência 6 + A.18.1.1; A.18.1.4	Pode ser considerada uma alternativa, redigir informações pessoais.	86.º	Tratamento e acesso do público aos documentos oficiais	Dados pessoais em documentos oficiais podem ser divulgados caso as mesmas sejam divulgadas sob as leis do tipo “liberdade de informação”.
Exigência 6 + A.18.1.1; A.18.1.4	Números de identificação nacional podem ser usados como autenticadores pessoais. Nesse caso, devem permanecer confidenciais para reduzir o risco de roubo de identidade. Sendo informações pessoais sensíveis, implica métodos de criptografia e/ou outros controlos de segurança.	87.º	Tratamento do número de identificação nacional	Podem impor controlos de privacidade para números de identificação nacionais.

Exigência 6 + A.18.1.1; A.18.1.4	Leis de trabalho podem-se cruzar com o RGPD e a privacidade, complicando ainda mais a conformidade, levando ao aparecimento de riscos.	88.º	Tratamento no contexto laboral	Podem impor restrições adicionais no tratamento corporativo, como a salvaguarda da dignidade humana e dos seus direitos.
Exigência 6 + A.18.1.4	Garantias de privacidade permanecem enquanto os titulares dos dados estiverem vivos. Enquanto isso, os riscos devem ser identificados, avaliados e tratados de maneira normal.	89.º	Garantias e derrogações relativas ao tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos	Dados pessoais arquivados para fins estatísticos devem ser tratados por meio de controlos, como a pseudonimização e minimização de dados, sempre que possível.
Exigência 6 + A.18.1.1; A.18.1.4	Leis de confidencialidade podem-se cruzar com o RGPD e a privacidade, complicando ainda mais a conformidade, levando ao aparecimento de riscos.	90.º	Obrigações de sigilo	Podem determinar leis adicionais sobre confidencialidade e obrigações de privacidade.
A.18.1.4	Privacidade e proteção de informação de caracter pessoal.	91.º	Normas vigentes em matéria de proteção dos dados das igrejas e associações religiosas	Normas de privacidade pré-existentes para igrejas e associações religiosas podem continuar, desde que estejam em acordo com o RGPD.
CAPÍTULO X - ATOS DELEGADOS E ATOS DE EXECUÇÃO				
A.18.1.1	Não relevante para os tratos de privacidade de uma organização. Exceto na medida em que precisem de cumprir as leis e regulamentos no qual são aplicáveis.	92.º	Exercício da delegação	Ter preocupação com a forma como o RGPD está a ser determinado pela União Europeia.
		93.º	Procedimento de comité	
CAPÍTULO XI - DISPOSIÇÕES FINAIS				
		94.º	Revogação da Diretiva 95/46/CE	

A.18.1.1	Não relevante para os tratos de privacidade de uma organização. Exceto na medida em que precisem de cumprir as leis e regulamentos no qual são aplicáveis.	95.º	Relação com a Diretiva 2002/58/CE	Ter preocupação com a forma como o RGPD está a ser determinado pela União Europeia.
		96.º	Relação com acordos celebrados anteriormente	
		97.º	Relatórios da Comissão	
		98.º	Revisão de outros atos jurídicos da União em matéria de proteção de dados	
		99.º	Entrada em vigor e aplicação	

Anexo 2 – Verificação e análise de ameaças

Tipo de evento	Ameaça	Origem *(*)*			GP/GI *(**)*
		A	I	N	
Danos físicos	Incêndio	✓	✓	✓	3/8
	Inundação (Danos causados pela água)	✓	✓	✓	3/8
	Poluição	✓	✓	✓	3/8
	Resíduos de poeira	✓	✓	✓	4/8
	Danificação intencional (Vandalismo)	✓	✓		5/4
	Destruição de equipamentos ou meios	✓	✓		7/3
	Adulteração/*Hackers* maliciosos (Sabotagem)	✓	✓		6/4
	Quebra no acesso à internet	✓	✓		6/4
	Acesso físico não autorizado (Intrusão)		✓		7/7
	Quebra na rede local	✓	✓		6/4
	Quebra/Sobrecarga de corrente elétrica	✓	✓	✓	6/3

Danos Natural	Fenómenos meteorológicos			✓	3/7
	Cheias			✓	5/8
	Terramoto			✓	3/9
	Tsunami			✓	2/10
	Sismo			✓	4/7
Falhas técnicas	Equipamento com deformação	✓			5/4
	Mau funcionamento do equipamento	✓			6/3
	Saturação do sistema de informação	✓	✓		5/5
	Erros de *software*	✓			9/1
	Falhas técnicas	✓			5/7
	Quebra na manutenção do sistema de informação	✓	✓		5/6
Tragédia	Guerra nuclear		✓		2/10
Acessos não autorizados	Utilização de software falsificado	✓	✓		6/7
	Obter cópias fraudulentas de software		✓		5/7

	Instalação de software não autorizado		✓		5/6
	Utilização de software não autorizado		✓		5/4
	Tratamento ilegal de dados		✓		6/4
	Corrupção de dados		✓		6/6
	Utilização não autorizada de equipamentos		✓		5/3
	Destruição de equipamentos		✓		4/5
	Apoderamento indevido de informação		✓		8/4
	Acesso não autorizado ao sistema		✓		7/4
Comprometimento de funções	Abuso e/ou falsificação de direitos	✓	✓		6/5
	Erros humanos	✓	✓		9/4
	Indisponibilidade dos RH	✓	✓	✓	6/5
	Recusa de ações		✓		3/8
	Indisponibilidade de pessoal	✓	✓	✓	8/5
Comprometimento da informação	Ações fraudulentas (adulteração de *software*/*hardware*)		✓		6/5

	Sniffing[24]		✓		6/2
	Espionagem		✓		5/4
	Roubo de documentos/equipamentos/midia				
	Violação de propriedade intelectual	✓	✓		8/5
	Divulgação não autorizada	✓	✓		7/4
	Divulgação de informação sigilosa	✓	✓		6/6
	Destruição de informação (ex. registos)	✓	✓		5/7
	Inserção de vírus	✓	✓		7/4
	Recuperação de informação descartada		✓		7/7
	Sinais de interferência		✓		7/3
	Atos de engenharia social[25]		✓		6/7

(*) A (Acidental); I (Intencional); N (Natural)
(**) GP (Grau de Probabilidade); GI (Grau de Impacto)

[24] Designados por escutas, os *hackers* usam *sniffers* para roubar dados, espionar o tráfego da rede e recolher informações sobre utilizadores. Disponível em: (https://www.avast.com/pt-br/c-sniffer) (Consultado em 20-04-2020)

[25] Processo de tentar convencer alguém de algo fictício, usando interações que podem revestir várias formas: mensagens de correio eletrónico, interações através das redes sociais ou mesmo chamadas telefónicas. Utilizam técnicas como pesquisas de informação descartada, espionagem, escuta não autorizada de chamadas, obtenção de informações através da proximidade, *fake news*, mensagens não solicitadas (*pop-ups*, *spam-mail*, *phishing*, *smishing*, *vishing*), *software* malicioso (*malware*), *pharming*, *footprinting*. Disponível em: (https://www.cncs.gov.pt/engenharia-social/) (Consultado em 20-04-2020)

Anexo 3 – Lista de verificação de auditoria

Lista de Verificação de auditoria				
Área de auditoria: Gestão da Segurança da Informação				Estado
Norma: ISO/ IEC 27001:2013			Motivo de auditoria: Avaliação da normalização afeta às atividades da empresa	
Políticas de Segurança da Informação				
A.5	5.1	Gestão da direção para a segurança da informação		
	5.1.1	Políticas para segurança da informação	Verificar: - Se existe uma política de segurança da informação; -Se a política foi aprovada pela gerência; -Se a política foi publicada e comunicada aos funcionários e partes externas relevantes.	**IM**
	5.1.2	Revisão das políticas de segurança da informação	Verificar: - Se as políticas de segurança da informação devem ser revisadas em intervalos planeados; - Se ocorre, mudanças significativas para garantir a sua contínua adequação, eficácia e eficácia.	**IM**
Organização da Segurança da Informação				
A.6	6.1	Organização Interna		
	6.1.1	Funções e responsabilidades de segurança da informação	Verificar se todas as responsabilidades de segurança da informação estão definidas e alocadas.	**IM**
	6.1.2	Segregação de deveres	Verificar se deveres conflitantes e áreas de responsabilidade estão segregados para reduzir as oportunidades de modificação não autorizada ou não intencional ou uso indevido dos ativos da organização.	**IM**

	6.1.3	Contacto com as autoridades	Verificar se foram mantidos contactos adequados com as autoridades relevantes.	**IM**
	6.1.4	Contacto com grupos de interesse especiais	Verificar se foram mantidos contactos adequados com grupos de interesses especiais ou outros fóruns especializados em segurança e associações profissionais.	**IM**
	6.1.5	Segurança da informação na gestão de projetos	Verificar se a segurança da informação é abordada na gestão de projetos, independentemente do tipo de projeto.	**IM**
	6.2	Dispositivos móveis e *"teleworking"*		
	6.2.1	Política de dispositivo móvel	Verificar se existe a adoção de uma política e medidas de segurança de apoio, adotadas para gerir os riscos introduzidos pelo uso de dispositivos móveis.	**IM**
	6.2.2	Teletrabalho	Verificar se há uma política e implementação de medidas de apoio de segurança para proteger as informações acedidas, processadas ou armazenadas nos locais de *"teleworking"*.	**IM**
Segurança nos Recursos Humanos				
A.7	7.1	Antes da contratação		
	7.1.1	Triagem	Verificar se foram realizadas verificações de antecedentes em todos os candidatos ao emprego, devem ser realizadas de acordo com as leis, regulamentos e éticas relevantes e devem ser proporcionais aos requisitos de negócios, à classificação das informações a serem acedidas e aos riscos percebidos.	**IM**
	7.1.2	Termos e condições de emprego	Verificar se os acordos contratuais com funcionários e contratados indicam as suas responsabilidades e a organização pela segurança das informações.	**PI**
	7.2	Durante a contratação		

	7.2.1	Responsabilidades de gestão	Verificar se existe um processo de gestão que assegura que todos os funcionários, contratados e terceiros executem as suas funções aplicando a segurança da informação de acordo com os procedimentos da organização.	**IM**
	7.2.2	Conscientização, educação e treinamento em segurança da informação	Verificar se todos os funcionários da organização e contratados recebem educação e formações apropriadas para a conscientização e atualizações regulares nos procedimentos organizacionais, relevantes para sua função.	**IM**
	7.2.3	Processo disciplinar	Verificar se existe um processo disciplinar formal contra funcionários que cometeram uma violação de segurança da informação.	**IM**
	7.3	Encerramento ou mudança da contratação		
	7.3.1	Rescisão ou mudança de responsabilidades do emprego	Verificar se as responsabilidades para a realização do termino ou mudança de emprego estão claramente definidos e documentados.	**NI**
Gestão de Ativos				
A.8	8.1	Responsabilidade dos ativos		
	8.1.1	Inventário de ativos	Verificar: - Se os ativos associados à informação e ao processamento de informação estão identificados; - Se existe um inventário desses ativos.	**IM**
	8.1.2	Propriedade de ativos	Verificar se há a atualização dos ativos.	**PI**
	8.1.3	Uso aceitável de ativos	Verificar: - Se existem adoção de regras para o uso aceitável de informações; - Se há ativos associados com instalações de informação e processamento de informações identificadas, documentadas e implementadas.	**NI**

	8.1.4	Retorno de ativos	Verificar se todos os funcionários e utilizadores externos devem devolver todos os ativos organizacionais em sua posse após o término da sua contratação.	**NA**
	8.2	Classificação da informação		
	8.2.1	Classificação da informação	Verificar se as informações devem ser classificadas em termos de requisitos legais, valor, criticidade e sensibilidade à divulgação não autorizada.	**IM**
	8.2.2	Rotulagem de informações	Verificar se existe um conjunto apropriado de procedimentos para a classificação de informações; - Se há desenvolvimento e implementação de acordo com as informações e esquemas de classificação adotado pela organização.	**NI**
	8.2.3	Manuseamento de ativos	Verificar se os procedimentos para a manipulação de ativos devem ser desenvolvidos e implementados em conformidade com o sistema de classificação da informação adotado pela organização.	**NI**
	8.3	Manuseamento de suporte de dados amovíveis		
	8.3.1	Gestão de mídia removível	Verificar se estão implementados procedimentos para a gestão de meios de comunicação de acordo com o sistema de classificação adotado pela organização.	**NA**
	8.3.2	Eliminação de mídia	Verificar se o material é excluído com segurança quando não for mais necessário, usando procedimentos formais.	**NA**
	8.3.3	Transferência de mídia física	Verificar se os meios de comunicação que contêm informações foram protegidos contra acessos, usos indevidos ou corrupção durante o transporte.	**NA**
Controlo de Acessos				
A.9	9.1	Requisitos de negócios de controlo de acesso		

	9.1.1	Política de controlo de acesso	Verificar se existe uma política de controlo de acesso a ser estabelecida, documentada e atualizada com base nos requisitos de negócios e segurança da informação.	**IM**
	9.1.2	Acesso a redes e serviços de rede	Verificar se os utilizadores têm acesso à rede e à rede de serviços especificamente autorizados a usar.	**IM**
	9.2	Requisitos de negócios de controlo de acesso		
	9.2.1	Registo e cancelamento de registo do utilizador	Verificar se existe um processo formal de registo e cancelamento do mesmo, implementado para permitir a atribuição de direitos de acesso.	**IM**
	9.2.2	Provisionamento de acesso do utilizador	Verificar se existe um registo formal de utilizador em vigor para a concessão e revogação do acesso a todos os sistemas de informação e serviços.	**IM**
	9.2.3	Gestão de direitos de acesso privilegiados	Verificar se existe a alocação e uso de direitos de acesso privilegiados a serem restritos e controlados.	**IM**
	9.2.4	Gestão de informações de autenticação secreta dos utilizadores	Verificar se a alocação de informações de autenticação deve ser controlada através de um processo formal de gestão.	**IM**
	9.2.5	Revisão dos direitos de acesso do utilizador	Verificar se os proprietários dos ativos, retificam os direitos de acesso dos utilizadores em intervalos regulares.	**NA**
	9.2.6	Remoção ou ajuste de direitos de acesso	Verificar se os direitos de acesso de todos os funcionários e utilizadores externos a instalações de processamento de informações e informações serão removidas após o término da contratação.	**IM**
	9.3	Responsabilidades dos utilizadores		
	9.3.1	Uso de informações de autenticação secreta	Verificar se os utilizadores estão a seguir as práticas da organização no uso de informações de autenticação.	**NA**

	9.4	Controlo de acessos aos sistemas e aplicativos		
	9.4.1	Restrição de acesso à informação	Verificar se o acesso às funções do sistema de informação e aplicativos deve ser restrito de acordo com a política de controlo de acesso.	**IM**
	9.4.2	Procedimentos seguros de ínicio de sessão	Verificar se a política de controlo de acesso, o acesso aos sistemas e os pedidos devem ser controlados por um procedimento seguro de *log-on*.	**NI**
	9.4.3	Sistema de gestão de senhas	Verificar se os sistemas de gestão de senhas garantem senhas de qualidade.	**NI**
	9.4.4	Uso de programas utilitários privilegiados	Verificar: - Se existe o uso de programas utilitários; - Se existe a sobreposição de controlos de sistema e aplicações restritas e controladas de forma rigida.	**NI**
	9.4.5	Controlo de acesso ao código fonte do programa	Verificar se o acesso ao código fonte do programa é restrito.	**IM**
Criptografia				
A.10	10.1	Controlos Criptográficos		
	10.1.1	Política de uso de controlos criptográficos	Verificar se foi desenvolvida e implementada uma política sobre o uso de controlos criptográficos para proteção da informação.	**NI**
	10.1.2	Gestão de chaves	Verificar se existe implantada uma política sobre o uso, a proteção e a vida útil das chaves criptográficas durante todo o ciclo de vida.	**NI**
Segurança Física e Ambiental				
A.11	11.1	Áreas seguras		

	11.1.1	Perímetro de segurança física	Verificar se existem perímetros de segurança para proteger áreas que contenham informações e instalações de processamento de informação (paredes, portões de entrada controlados por cartão ou receções).	**NI**
	11.1.2	Controlos físicos de entrada	Verificar se as áreas seguras estão protegidas por entradas controladas apropriadas para garantir que apenas o pessoal autorizado tenha acesso.	**NI**
	11.1.3	Segurança em escritórios, salas e instalações	Verificar se existem medidas de segurança física de escritórios, salas e instalações.	**IM**
	11.1.4	Proteção contra ameaças externas e ambientais	Verificar se existe medidas de proteção física contra desastres naturais (incêndios, inundações, terremoto, explosão, distúrbios civis), ataques maliciosos ou acidentes.	**PI**
	11.1.5	Trabalhar em áreas seguras	Verificar se foram aplicados procedimentos e diretrizes para trabalhar em áreas seguras.	**PI**
	11.1.6	Áreas de entrega e carregamento	Verificar se existem pontos de acesso, como áreas de entrega e carga e outros pontos onde pessoas não autorizadas podem entrar no local controlado para evitar acesso não autorizado.	**NI**
	11.2	Equipamento		
	11.2.1	Localização e proteção de equipamentos	Verificar se estão instalados equipamentos para reduzir os riscos de ameaças, perigos ambientais e oportunidades de acesso não autorizado.	**IM**
	11.2.2	Utilitários de suporte	Verificar se o equipamento está protegido contra falhas de energia e/ou rede e outras interrupções causadas por falhas no suporte a utilizadores.	**NI**
	11.2.3	Segurança de cablagem	Verificar se existe proteção contra a intercetação, interferência ou danos nos cabos de energia e telecomunicações que transportam dados ou suportam serviços de informação.	**IM**

	11.2.4	Manutenção de Equipamento	Verificar se o equipamento está corretamente conservado para garantir a sua continuidade, disponibilidade e integridade.	**IM**
	11.2.5	Remoção de ativos	Verificar se existe um procedimento para garantir que os equipamentos, informações ou software não devem ser retirados do local sem autorização prévia.	**IM**
	11.2.6	Segurança de equipamentos e ativos externos	Verificar se a segurança está aplicada aos ativos externos, levando em consideração os diferentes riscos de trabalhar fora das instalações da organização.	**NA**
	11.2.7	Eliminação ou reutilização segura de equipamentos	Verificar se todos os itens do equipamento que contêm mídias de armazenamento foram verificados para que quaisquer dados confidenciais e software licenciado tenha sido removido com segurança antes de serem eliminados ou reutilizados.	**IM**
	11.2.8	Equipamento de utilizador autónomo	Verificar se os utilizadores garantem que o equipamento não assistido tenha proteção.	**NI**
	11.2.9	Política de mesa clara e tela clara	Verificar: - Se existe um arquivamento de documentos e mídias de armazenamento removível; - Se existe adoção do *"clear screen"* para instalações de processamento de informações.	**IM**
Segurança nas operações				
A.12	12.1	Procedimentos e responsabilidades operativas		
	12.1.1	Procedimentos operativos documentados	Verificar se os procedimentos operativos foram documentados e disponibilizados a todos os utilizadores que precisam deles.	**PI**

	12.1.2	Gestão de alterações	Verificar se foram controladas as alterações na organização, processos de negócios, processamento de informações, instalações e sistemas que afetam a segurança da informação.	**PI**
	12.1.3	Gestão de capacidade	Verificar se os usos de recursos foram, ajustados e projetados requisitos de capacidade futura para garantir o desempenho do sistema.	**NI**
	12.1.4	Separação de ambientes de desenvolvimento, teste e operativos	Verificar se o desenvolvimento e teste foram separados para reduzir os riscos de acesso não autorizado ou alterações nos sistemas operativos.	**IM**
	12.2	Proteção contra *malware*		
	12.2.1	Controlos contra *malware*	Verificar se estão implementados os controlos de deteção, prevenção e recuperação para proteção contra *malware*.	**IM**
	12.3	*Backup*		
	12.3.1	Backup de informações	Verificar se existe um processo para assegurar que as cópias de segurança de informação, software e imagens do sistema foram executadas e testadas regularmente de acordo com a política de backup?	**NI**
	12.4	*Login* e Monitorização		
	12.4.1	Registo de eventos	Verificar se existem registos de auditoria das atividades de utilizadores, exceções, eventos de segurança da informação, falhas e informações de utilizadores.	**IM**
	12.4.2	Proteção de informações de log	As informações e sistemas de log protegidos estão protegidos contra falsificação e acesso não autorizado?	**IM**
	12.4.3	Logs de administrador e operador	Verificar se as atividades de administrador e operador do sistema estão registados e os logs protegidos e atualizados.	**NI**

	12.4.4	Sincronização do relógio	Verificar se os relógios de todos os sistemas de informação relevantes, dentro de uma organização ou domínio de segurança estão sincronizados com uma fonte de tempo precisa.	**IM**
	12.5	Controlo de *software* operativo		
	12.5.1	Instalação de software em sistemas de produção	Verificar se existem procedimentos para controlar a instalação do software nos sistemas de produção.	**IM**
	12.6	Gestão de vulnerabilidades técnicas		
	12.6.1	Gestão de vulnerabilidades técnicas	Verificar se existem informações sobre vulnerabilidades técnicas de sistemas de informação, apropriadas para abordar o risco associado.	**PI**
	12.6.2	Restrições na instalação do software	Verificar se as regras que regem a instalação do software pelos utilizadores estão implementadas.	**NI**
	12.7	Considerações sobre auditoria de sistemas de informação		
	12.7.1	Controlos de auditoria de sistemas de informação	Verificar se os requisitos e atividades de auditoria que envolvam a verificação nos sistemas de produção devem ser planeados e acordados para minimizar as interrupções nos processos de negócios.	**IM**
Segurança nas Comunicações				
A.13	13.1	Gestão na segurança das redes		
	13.1.1	Controlos de rede	Verificar se as redes foram geridas e controladas, com o intuito de proteger (ameaças) as informações em sistemas e aplicações que utilizem a rede.	**IM**

	13.1.2	Segurança de serviços de rede	Verificar: - Se existem mecanismos de segurança, níveis de serviço e requisitos de gestão de todos os serviços de rede; - Se foram identificados e incluídos acordos de serviços de rede; - Se esses serviços são fornecidos internamente ou terceirizados.	**IM**
	13.1.3	Segregação em redes	Verificar se grupos de serviços de informação, utilizadores e sistemas de informação foram separados em redes.	**IM**
	13.2	Transferência de informação		
	13.2.1	Políticas e procedimentos de transferência de informações	Verificar se existem procedimentos e controlos formais de transferência, para proteção da transferência de informações, através da utilização de todos os tipos de meios de comunicação.	**NA**
	13.2.2	Acordos sobre transferência de informações	Verificar se foram adotados acordos para a transferência segura de informações comerciais entre a organização e as partes externas.	**NA**
	13.2.3	Mensagens eletrónicas	Verificar se as informações envolvidas nas mensagens eletrónicas estão devidamente protegidas.	**PI**
	13.2.4	Acordos de confidencialidade ou não divulgação	Verificar se existem requisitos para acordos de confidencialidade ou não divulgação, refletindo as necessidades da organização para a proteção de informações.	**IM**
Aquisição, Desenvolvimento e Manutenção de Sistemas				
A.14	14.1	Requisitos de segurança dos sistemas de informação		
	14.1.1	Análise e especificação de requisitos de segurança da informação	Verificar se os requisitos relacionados com a segurança da informação estão incluídos nos requisitos para novos sistemas de informação ou aprimoramentos nos sistemas de informação existentes.	**IM**

	14.1.2	Proteger serviços de aplicativos em redes públicas	Verificar se as informações envolvidas nos serviços de aplicativos que passam por redes públicas estão contra atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas.	**IM**
	14.1.3	Proteger transações de serviços de aplicativos	Verificar se as informações envolvidas nas transações de serviços de aplicativos foram protegidas para evitar a transmissão incompleta, navegação incorreta, alteração, divulgação, duplicação não autorizada de mensagens.	**IM**
	14.2	Segurança nos processos de suporte e desenvolvimento		
	14.2.1	Política de desenvolvimento seguro	Verificar se as regras para o desenvolvimento de *software* e sistemas foram estabelecidas e aplicadas aos desenvolvimentos dentro da organização.	**PI**
	14.2.2	Procedimentos de controle de alterações do sistema	Verificar se as alterações nos sistemas do ciclo de vida de desenvolvimento foram controladas pelo uso de procedimentos formais de controlo de alterações.	**IM**
	14.2.3	Revisão técnica de aplicativos após alterações na plataforma operativa	Verificar: - Se as plataformas operativas foram alteradas; - Se os aplicativos críticos para os negócios foram revistos e testados para garantir que não haja impacto adverso nas operações ou na segurança organizacional.	**IM**
	14.2.4	Restrições sobre mudanças nos pacotes de software	Verificar se as modificações nos pacotes de *software* foram limitadas a mudanças necessárias e todas as mudanças devem ser rigorosamente controladas.	**IM**
	14.2.5	Princípios de engenharia de sistemas seguros	Verificar se os princípios para engenharia de sistemas seguros estão estabelecidos, documentados, mantidos e aplicados a quaisquer esforços de implementação nos sistemas de informação.	**IM**

	14.2.6	Ambiente de desenvolvimento seguro	Verificar se a organização estabelece e protege adequadamente a segurança do ambiente de desenvolvimento e integração de sistemas, que cobrem todo o ciclo de vida do desenvolvimento do sistema.	**IM**
	14.2.7	Desenvolvimento terceirizado	Verificar se a organização supervisiona e monitoriza as atividades de desenvolvimento de sistemas terceirizados.	**NA**
	14.2.8	Teste de segurança do sistema	Verificar se o teste da funcionalidade de segurança é realizado durante o desenvolvimento.	**IM**
	14.2.9	Teste de aceitação do sistema	Verificar se os programas de teste de aceitação e critérios relacionados estão estabelecidos para novos sistemas de informação, atualizações e novas versões.	**IM**
	14.3	Dados de teste		
	14.3.1	Proteção de dados de teste	Verificar se os dados de teste são selecionados cuidadosamente, protegidos e controlados.	**NA**
Relações com Fornecedores				
A.15	15.1	Segurança da informação nos relacionamentos com fornecedores		
	15.1.1	Política de segurança da informação para relacionamentos com fornecedores	Verificar se os requisitos de segurança da informação para atenuar os riscos, (associados ao acesso do fornecedor aos ativos da organização) foram acordados com o fornecedor e documentados.	**NI**
	15.1.2	Abordar a segurança nos contratos com fornecedores	Verificar se todos os requisitos de segurança da informação estão estabelecidos e acordados com cada fornecedor, para que se possa aceder, processar, armazenar, comunicar ou fornecer componentes da infraestrutura de TI para as informações da organização.	**NI**

	15.1.3	Cadeia de suprimentos de tecnologia da informação e comunicação	Verificar se os acordos com fornecedores incluem requisitos para tratar dos riscos de segurança da informação, associados aos serviços de tecnologia da informação, comunicação e produtos.	**PI**
	15.2	Gestão da entrega de serviços a fornecedores		
	15.2.1	Monitorização e revisão de serviços de fornecedores	Verificar se a organização monitoriza, revista e audita regularmente a prestação de serviços do fornecedor.	**NA**
	15.2.2	Gestão de alterações nos serviços do fornecedor	Verificar se as mudanças na prestação de serviços pelos fornecedores, incluindo a manutenção e melhoria das políticas, procedimentos e controlos de segurança da informação existentes, foram geridas, levando em consideração a criticidade das informações, sistemas, processos de negócios envolvidos e a reavaliação dos riscos.	**NI**
Gestão de Incidentes na Segurança da Informação				
A.16	16.1	Gestão de incidentes e melhorias na segurança da informação		
	16.1.1	Responsabilidades e procedimentos	Verificar se as responsabilidades e procedimentos de gestão foram estabelecidos, para garantir uma resposta rápida, eficaz e ordenada aos incidentes de segurança da informação.	**NI**
	16.1.2	Reportar eventos de segurança da informação	Verificar se os eventos de segurança da informação são relatados através dos canais de gestão apropriados, o mais rápido possível.	**IM**

	16.1.3	Reportar falhas de segurança da informação	Verificar se os funcionários e contratados que usam os sistemas e serviços de informação da organização observam e relatam quaisquer deficiências observadas ou suspeitas de segurança das informações nos sistemas ou serviços.	**IM**
	16.1.4	Avaliação e decisão sobre eventos de segurança da informação	Verificar se os eventos de segurança da informação são avaliados e decididos se devem ser classificados como incidentes de segurança da informação.	**IM**
	16.1.5	Resposta a incidentes de segurança da informação	Verificar se os incidentes de segurança da informação são respondidos de acordo com os procedimentos documentados.	**IM**
	16.1.6	Aprender com incidentes de segurança da informação	Verificar se o conhecimento adquirido com a análise e resolução de incidentes de segurança da informação, são usados para reduzir a probabilidade ou o impacto de incidentes futuros.	**IM**
	16.1.7	Recolha de evidências	Verificar se a organização define e aplica procedimentos para a identificação, recolha, aquisição e preservação de informações, que podem servir como evidência.	**IM**
Aspetos de Segurança da Informação na Gestão da Continuidade de Negócios				
A.17	17.1	Continuidade da segurança da informação		
	17.1.1	Planeamento da continuidade da segurança da informação	Verificar se a organização determina requisitos de segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, como por exemplo durante uma crise ou desastre.	**IM**

	17.1.2	Implementação da continuidade da segurança da informação	Verificar se a organização estabelece, documenta, implementa e mantém processos, procedimentos e controlos para garantir o nível de continuidade necessário para a segurança da informação durante uma situação adversa.	**NI**
	17.1.3	Verificar, revisar e avaliar a continuidade da segurança da informação	Verificar se a organização adquire os controlos de continuidade de segurança da informação estabelecidos e implementados em intervalos regulares, a fim de garantir que sejam válidos e eficazes em situações adversas.	**NI**
	17.2	Redundâncias		
	17.2.1	Disponibilidade de instalações de processamento de informações	Verificar se as instalações de processamento de informações são implementadas com redundância suficiente para atender aos requisitos de disponibilidade.	**IM**
Conformidade				
A.18	18.1	Cumprimento dos requisitos legais e contratuais (leis e contratos de lei)		
	18.1.1	Identificação da legislação aplicável e requisitos contratuais	Verificar se todos os requisitos estatutários, regulamentares, contratuais e legislativos relevantes e a abordagem da organização para atender a esses requisitos são explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação e organização.	**IM**
	18.1.2	Direito de propriedade intelectual	Verificar se foram implantados procedimentos, para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados aos direitos de propriedade intelectual e ao uso de produtos de software proprietários.	**NI**

	18.1.3	Proteção de registos	Verificar se os registos são protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos legislativos, regulamentares, contratuais e comerciais.	**IM**
	18.1.4	Privacidade e proteção de informações de identificação pessoal	Verificar se a privacidade e a proteção das informações de identificação pessoal, são garantidas conforme exigido na legislação e regulamentação relevantes, quando aplicável.	**IM**
	18.1.5	Regulação dos controles criptográficos	Verificar se os controlos criptográficos são utilizados em conformidade com todos os acordos, leis e regulamentos relevantes.	**NA**
	18.2	Revisões de segurança da informação		
	18.2.1	Revisão independente da segurança da informação	Verificar se a abordagem da organização para gerir a segurança da informação e a sua implementação (ou seja, objetivos, políticas, processos e procedimentos de controlo da segurança da informação) são revistas, independentemente em intervalos planeados ou quando ocorrem alterações significativas.	**NA**
	18.2.2	Conformidade com políticas e normas de segurança	Verificar se os gerentes revisam regularmente a conformidade do processamento e dos procedimentos de informações na sua área de responsabilidade com as políticas, padrões e quaisquer outros requisitos de segurança adequados.	**IM**
	18.2.3	Revisão da conformidade técnica	Verificar se os sistemas de informação são revisados regularmente quanto à conformidade com as políticas e padrões de segurança da informação da organização.	**IM**

Anexo 4 – Observação do funcionamento da empresa

Lista de Verificação de auditoria				
				Realizada na data: **06/01/2020**
Área de auditoria: Gestão da Segurança da Informação				Considerações
Norma: ISO/ IEC 27001:2013			Motivo de auditoria: Avaliação da normalização afeta às atividades da empresa	
Políticas de Segurança da Informação				
A.5	5.1	Gestão da direção para a segurança da informação		
	5.1.1	Políticas para segurança da informação	Verificar: - Se existe uma política de segurança da informação; -Se a política foi aprovada pela gerência; -Se a política foi publicada e comunicada aos funcionários e partes externas relevantes.	Obs.: A política existe e foi aprovada.
	5.1.2	Revisão das políticas de segurança da informação	Verificar: - Se as políticas de segurança da informação devem ser revisadas em intervalos planeados; - Se ocorre, mudanças significativas para garantir a sua contínua adequação, eficácia e eficácia.	Obs.: A política de segurança é atualizada anualmente.
Organização da Segurança da Informação				
A.6	6.1	Organização Interna		

	6.1.1	Funções e responsabilidades de segurança da informação	Verificar se todas as responsabilidades de segurança da informação estão definidas e alocadas.	Sem observações.
	6.1.2	Segregação de deveres	Verificar se deveres conflitantes e áreas de responsabilidade estão segregados para reduzir as oportunidades de modificação não autorizada ou não intencional ou uso indevido dos ativos da organização.	Sem observações.
	6.1.3	Contacto com as autoridades	Verificar se foram mantidos contactos adequados com as autoridades relevantes.	Sem observações.
	6.1.4	Contacto com grupos de interesse especiais	Verificar se foram mantidos contactos adequados com grupos de interesses especiais ou outros fóruns especializados em segurança e associações profissionais.	Sem observações.
	6.1.5	Segurança da informação na gestão de projetos	Verificar se a segurança da informação é abordada na gestão de projetos, independentemente do tipo de projeto.	Sem observações.
	6.2	Dispositivos móveis e *"teleworking"*		
	6.2.1	Política de dispositivo móvel	Verificar se existe a adoção de uma política e medidas de segurança de apoio, adotadas para gerir os riscos introduzidos pelo uso de dispositivos móveis.	Atualmente existe ligação interna e externa. No entanto, em ambas estão implementadas medidas e padrões de segurança. Existe a rede *guest*, que só é possível ser acedida através do uso de login e password. Obs.: Não é possível ligarem-se à rede interna através de equipamentos exteriores.

	6.2.2	Teletrabalho	Verificar se há uma política e implementação de medidas de apoio de segurança para proteger as informações acedidas, processadas ou armazenadas nos locais de *"teleworking"*.	O servidor está exposto, apenas quem tem acesso através de um utilizador e palavra passe é que consegue aceder a aplicação. Acesso interno acedida por uma VPN, limitado a qualquer pessoa.
Segurança nos Recursos Humanos				
A.7	7.1	Antes da contratação		
	7.1.1	Triagem	Verificar se foram realizadas verificações de antecedentes em todos os candidatos ao emprego, devem ser realizadas de acordo com as leis, regulamentos e éticas relevantes e devem ser proporcionais aos requisitos de negócios, à classificação das informações a serem acedidas e aos riscos percebidos.	Obs.: Na IL é necessário fazer todo o tipo de rastreio que ilegalmente ou legalmente se possa realizar.
	7.1.2	Termos e condições de emprego	Verificar se os acordos contratuais com funcionários e contratados indicam as suas responsabilidades e a organização pela segurança das informações.	Sem observações.
	7.2	Durante a contratação		
	7.2.1	Responsabilidades de gestão	Verificar se existe um processo de gestão que assegura que todos os funcionários, contratados e terceiros executem as suas funções aplicando a segurança da informação de acordo com os procedimentos da organização.	Sem observações.
	7.2.2	Conscientização, educação e treinamento em segurança da informação	Verificar se todos os funcionários da organização e contratados recebem educação e formações apropriadas para a conscientização e atualizações regulares nos procedimentos organizacionais, relevantes para sua função.	Não sendo obrigatório, o "*onbording"* diz respeito aos departamentos, segurança, métodos de qualidade, responsabilidades e cargos. No entanto, caso não se cumpra com o requisito nº. 7.2.1 é obrigatório o cumprimento deste requisito.

	7.2.3	Processo disciplinar	Verificar se existe um processo disciplinar formal contra funcionários que cometeram uma violação de segurança da informação.	Se algo não for cumprido com o estabelecido no ponto 7.2.2, o processo disciplinar ativa-se.
	7.3	Encerramento ou mudança da contratação		
	7.3.1	Rescisão ou mudança de responsabilidades do emprego	Verificar se as responsabilidades para a realização do termino ou mudança de emprego estão claramente definidos e documentados.	Futuramente a implementar, será atualizado anualmente.
Gestão de Ativos				
A.8	8.1	Responsabilidade dos ativos		
	8.1.1	Inventário de ativos	Verificar: - Se os ativos associados à informação e ao processamento de informação estão identificados; - Se existe um inventário desses ativos.	Existe um inventário; O inventário contém toda a informação da organização que ajuda a fazer o pressuposto que a empresa tem: máquinas, *"access points*", ligações à internet e à informação organizacional, seja de bases de dados, seja de documentos digitais.
	8.1.2	Propriedade de ativos	Verificar se há a atualização dos ativos.	Sim, há atualização. No entanto, varia de acordo com a utilização que os utilizadores dão à aplicação, pois se, é uma aplicação não utilizada, não há necessidade de ser atualizada.
	8.1.3	Uso aceitável de ativos	Verificar: - Se existem adoção de regras para o uso aceitável de informações; - Se há ativos associados com instalações de informação e processamento de informações identificadas, documentadas e implementadas.	Não esta implementada, porque não há restrições na utilização de ativos. No entanto, não é possível a recolha exterior de ativos, desde equipamentos a dispositivos externos. Há apenas a VPN por parte do proprietário. Os funcionários estão proibidos de levar equipamentos para o exterior ou aceder à VPN da empresa no exterior.

	8.1.4	Devolução de ativos	Verificar se todos os funcionários e utilizadores externos devem devolver todos os ativos organizacionais em sua posse após o término da sua contratação.	(Ver 8.1.3) Se é proibida a utilização de equipamentos exteriores, conclui-se que não haverá a sua devolução.
	8.2	Classificação da informação		
	8.2.1	Classificação da informação	Verificar se as informações devem ser classificadas em termos de requisitos legais, valor, criticidade e sensibilidade à divulgação não autorizada.	Existem três níveis principais na empresa, sendo elas o Público, Interno e Confidencial (secreto e ultrassecreto). Nível Público - pode ser acedido por todos aqueles que não pertencem ao quadro, como exemplos temos a politica de segurança, politica de qualidade, ambos demonstrados como documentos públicos; Nível Interno - só para as pessoas internas à empresa, como exemplos temos as normas, procedimentos, processos, instruções de trabalho); Nível Confidencial - Agrega-se a parte administrativa, financeira, gestão de recursos humanos. Com os subníveis secreto e ultra-secreto, obriga a criação de uma sala NATO, que se refere a uma sala certificada pelo GNS (Gabinete Nacional de Segurança), da categoria NATO. Mais inf. https://www.ead.pt/gns-nato-secret/
	8.2.2	Rotulagem de informações	Verificar se existe um conjunto apropriado de procedimentos para a classificação de informações; - Se há desenvolvimento e implementação de acordo com as informações e esquemas de classificação adotado pela organização.	Não implementado, é uma falha. Pode vir a ser um problema sendo que tudo geral, porém nada está especificado. Obs.: não existe a efetivação de equipamentos como impressoras, deste modo, não se corre o risco do controlo de confidencialidade. Porém caso contrário deixaria de o ser.

	8.2.3	Manuseamento de ativos	Verificar se os procedimentos para a manipulação de ativos devem ser desenvolvidos e implementados em conformidade com o sistema de classificação da informação adotado pela organização.	Não implementado. Apenas etiquetado para o nível confidencial. Deste modo, os exemplos das informações contidas das bases de dados são confidenciais, não há procedimentos de organização de como se deve ser tratada essa informação.
	8.3	Manuseamento de suporte de dados amovíveis		
	8.3.1	Gestão de mídia removível	Verificar se estão implementados procedimentos para a gestão de meios de comunicação de acordo com o sistema de classificação adotado pela organização.	Não há dados amovíveis. Através da definição da BIOS de cada máquina, é detetado caso se insira qualquer dispositivo externo.
	8.3.2	Eliminação de mídia	Verificar se o material é excluído com segurança quando não for mais necessário, usando procedimentos formais.	Não aplicável; Não é necessário, não há utilização no exterior ou interior da empresa.
	8.3.3	Transferência de mídia física	Verificar se os meios de comunicação que contêm informações foram protegidos contra acessos, usos indevidos ou corrupção durante o transporte.	Não aplicável; Não há o transporte da informação.
Controlo de Acessos				
A.9	9.1	Requisitos de negócios de controlo de acesso		
	9.1.1	Política de controlo de acessos	Verificar se existe uma política de controlo de acesso a ser estabelecida, documentada e atualizada com base nos requisitos de negócios e segurança da informação.	A empresa ambiciona futuramente a implementar testes que permitam avaliar a segurança de um sistema de computador (***Pentesting***). Porém, após a avaliação, será realizado como método de *output,* um relatório para a entrega na mesma.
	9.1.2	Acesso a redes e serviços de rede	Verificar se os utilizadores têm acesso à rede e à rede de serviços especificamente autorizados a usar.	Utilizadores apenas têm acesso à rede interna.

	9.2	Requisitos de negócios de controlo de acesso		
	9.2.1	Registo e cancelamento de registo do utilizador	Verificar se existe um processo formal de registo e cancelamento do mesmo, implementado para permitir a atribuição de direitos de acesso.	Respetivamente à gestão de utilizadores, que corresponde à sua criação e eliminação, o administrador realiza a criação dos mesmos no "*onbording",* que se inicia assim que um candidato concorda em aceitar um emprego, desde a sua implantação ao seu sucesso na mesma. Já o "*offboarding*" refere-se à eliminação de um funcionário da empresa.
	9.2.2	Provisionamento de acesso do utilizador	Verificar se existe um registo formal de utilizador em vigor para a concessão e revogação do acesso a todos os sistemas de informação e serviços.	Sem observações.
	9.2.3	Gestão de direitos de acesso privilegiados	Verificar se existe a alocação e uso de direitos de acesso privilegiados a serem restritos e controlados.	A gestão de direitos é apenas realizada a cargo do Administrador.
	9.2.4	Gestão de informações de autenticação secreta dos utilizadores	Verificar se a alocação de informações de autenticação deve ser controlada através de um processo formal de gestão.	Conforme, onde a atribuição de uma informação secreta deve ser controlada através de um processo de modo de gestão. A política é reservada a restrições de criação (Caracteres maiúsculos e minúsculos, 8 caracteres no mínimo e inserção de caracteres especiais.
	9.2.5	Revisão dos direitos de acesso do utilizador	Verificar se os proprietários dos ativos, retificam os direitos de acesso dos utilizadores em intervalos regulares.	Na empresa, a verificação dos utilizadores realiza-se através das existências dos mesmos, analisar que o que consta nos RH é exatamente o mesmo que consta na tabela dos utilizadores (***AD***).
	9.2.6	Remoção ou ajuste de direitos de acesso	Verificar se os direitos de acesso de todos os funcionários e utilizadores externos a instalações de processamento de informações serão removidos após o término da contratação.	(Ver 9.2.1) Como não há acesso a equipamento externo, em termos de controlo de acesso procede-se através de uma VPN. Contudo, em casos de "*outsourcing*" o utilizador, conectado à VPN poderá deixar de ter acesso à mesma num dia programável (definido pelo Administrador). Por outras palavras,

				no caso de haver um contrato com uma entidade externa, é necessário fazer a remoção total do acesso, cumprindo com possíveis políticas.
	9.3	Responsabilidades dos utilizadores		
	9.3.1	Uso de informações de autenticação secreta	Verificar se os utilizadores estão a seguir as práticas da organização no uso de informações de autenticação.	Cada um tem as suas responsabilidades e passwords privadas. Não é aplicável o mesmo uso de sessões de utilizador ou passwords, devido posterior ao facto de depois não ser possível rastrear, como exemplo, ver quem eliminou certo ficheiro. Obs.: No caso de duas pessoas do mesmo departamento, ambas têm o mesmo acesso à informação, embora tenham sessões de utilizador diferentes.
	9.4	Controlo de acessos ao sistema e aplicativos		
	9.4.1	Restrição de acesso à informação	Verificar se o acesso às funções do sistema de informação e aplicativos devem ser restritos de acordo com a política de controlo de acesso.	Está ligada inteiramente à política de controlo de acessos. Desde que esteja estabelecido uma política de controlo de acessos, existe uma restrição. Os utilizadores apenas acedem ao que o administrador permitir, sem interferir com acesso ás informações confidenciais.
	9.4.2	Procedimentos seguros de início de sessão	Verificar se a política de controlo de acesso, o acesso aos sistemas e os pedidos devem ser controlados por um procedimento seguro de *log-on*.	Existe a política e os procedimentos, no entanto, o controlo não é verificado. A autenticação depende do que os utilizadores quiserem.

	9.4.3	Sistema de gestão de senhas	Verificar se os sistemas de gestão de senhas garantem senhas de qualidade.	(Ver 9.3.1) Não é implementado. Funciona da seguinte maneira: Conta criada pelo administrador; posteriormente enviada ao funcionário; este por sua vez irá mudar a password, conforme os critérios já mencionados anteriormente. Porém, além de haver uma política, não é feita uma verificação e validação da máquina para a definição da password, sendo de livre vontade a escolha da mesmo pelo utilizador.
	9.4.4	Uso de programas utilitários privilegiados	Verificar: - Se existe o uso de programas utilitários; - Se existe a sobreposição de controlos de sistema e aplicações restritas e controladas de forma rígida.	Não é implementado. O sistema operativo utilizado é o *Linux*, no entanto para a utilização de programas utilitários privilegiados seria necessário em cada máquina o utilizador saber manusear nos servidores e acessos informáticos para possível definição de privilégios de programas; necessário também ter acesso ao servidor.
	9.4.5	Controlo de acesso ao código fonte do programa	Verificar se o acesso ao código fonte do programa é restrito.	Necessário utilizar o ***SVN*** - sistema que permite colocar o código fonte. Numa máquina, cada utilizador tem o seu login de VPN. Um programa feito em grupo de trabalho por programadores será partilhado através das autorizações de compartilhamento da VPN e o administrador consegue através do *Upsource* (até 10 utilizadores a sua utilização é gratuita) controlar e aceitar as modificações realizadas até ao momento, vendo a data, hora e o autor da modificação.
Criptografia				
A.10	10.1	Controlos Criptográficos		

	10.1.1	Política de uso de controlos criptográficos	Verificar se foi desenvolvida e implementada uma política sobre o uso de controlos criptográficos para proteção da informação.	Em termos de software a informação está toda criptografada e organizada. No entanto, em relação à informação que corre dentro da empresa, existe um software partilhado por terceiros com informação criptografada (***ODOO***). Obs.: Informação sigilosa e confidencial está apenas na posse do administrador.
	10.1.2	Gestão de chaves	Verificar se existe implantada uma política sobre o uso, a proteção e a vida útil das chaves criptográficas durante todo o ciclo de vida.	Através do software utilizado anteriormente que faz a atualização das chaves criptográficas.
Segurança Física e Ambiental				
A.11	11.1	Áreas seguras		
	11.1.1	Perímetro de segurança física	Verificar se existem perímetros de segurança para proteger áreas que contenham informações e instalações de processamento de informação (paredes, portões de entrada controlados por cartão ou receções).	Sem observações.
	11.1.2	Controlos físicos de entrada	Verificar se as áreas seguras estão protegidas por entradas controladas apropriadas para garantir que apenas o pessoal autorizado tenha acesso.	Acesso autorizado através da entrada de porta com acesso a chaves. Obs.: No entanto em relação à circulação da informação, apenas o administrador tem acesso aos servidores.
	11.1.3	Segurança em escritórios, salas e instalações	Verificar se existem medidas de segurança física de escritórios, salas e instalações.	Associar as medidas de segurança do (11.1.2).
	11.1.4	Proteção contra ameaças externas e ambientais	Verificar se existe medidas de proteção física contra desastres naturais (incêndios, inundações,	As medidas de segurança contra incêndios e controlo da segurança está implementada no exterior do escritório.

			terremoto, explosão, distúrbios civis), ataques maliciosos ou acidentes.	
	11.1.5	Trabalhar em áreas seguras	Verificar se foram aplicados procedimentos e diretrizes para trabalhar em áreas seguras.	Obs.: A sala que abrange os servidores é considerada uma zona segura.
	11.1.6	Áreas de entrega e carregamento	Verificar se existem pontos de acesso, como áreas de entrega e carga e outros pontos onde pessoas não autorizadas podem entrar no local controlado para evitar acesso não autorizado.	Sem observações.
	11.2	Equipamento		
	11.2.1	Localização e proteção de equipamentos	Verificar se estão instalados equipamentos para reduzir os riscos de ameaças, perigos ambientais e oportunidades de acesso não autorizado.	Em relação aos perigos ambientais, os equipamentos tecnológicos não necessários para a empresa são eliminados, fazendo a substituição dos discos e vendendo o equipamento seja por inteiro ou peças através de uma declaração de venda, deixando desta forma de ser responsável pelo equipamento que estava em sua posse. Em relação aos riscos e ameaças, na empresa não é possível haver aquivos ou papelada, sendo tudo realizado digitalmente, a manutenção de arquivos em cima de mesas é proibida, exceto rascunhos do desenvolvimento de programas como esboços. Os computadores têm acesso a bloqueios automáticos a partir de 1 minuto sem utilização.
	11.2.2	Utilitários de suporte	Verificar se o equipamento está protegido contra falhas de energia e/ou rede e outras interrupções causadas por falhas no suporte a utilizadores.	Obs.: Responsável refere que foi um problema relevante, por eventuais falhas de energia mandarem os sistemas abaixo. Porém, haviam quadros para controlar os limites de energia.

	11.2.3	Segurança de cablagem	Verificar se existe proteção contra a intercetação, interferência ou danos nos cabos de energia e telecomunicações que transportam dados ou suportam serviços de informação.	Utilizam uma cablagem normal; em termos de rede, só era possível aceder num dispositivo exterior na empresa, através de uma identificação prévia no **MAC Address** da firewall.
	11.2.4	Manutenção de Equipamento	Verificar se o equipamento está corretamente conservado para garantir a sua continuidade, disponibilidade e integridade.	É mantido através de atualizações e manutenção periódica. No entanto havia controlo de todos os equipamentos e máquinas associadas a empresa, caso contrário não era possível aceder a *firewall*.
	11.2.5	Remoção de ativos	Verificar se existe um procedimento para garantir que os equipamentos, informações ou software não devem ser retirados do local sem autorização prévia.	Havia vigia e controlo da segurança dos equipamentos, sendo que só os funcionários poderiam trabalhar nos equipamentos que lhes eram entregues na empresa, dentro do horário definido.
	11.2.6	Segurança de equipamentos e ativos externos	Verificar se a segurança está aplicada aos ativos externos, levando em consideração os diferentes riscos de trabalhar fora das instalações da organização.	Sem observações (não se pode auditar).
	11.2.7	Eliminação ou reutilização segura de equipamentos	Verificar se todos os itens do equipamento que contêm mídias de armazenamento foram verificados para que quaisquer dados confidenciais e software licenciado tenha sido removido com segurança antes de serem eliminados ou reutilizados.	Caso um equipamento fosse excluído, era necessário fazer uma transferência segura de toda a informação para outro equipamento. Esse equipamento sofria uma formatação de baixo nível para posteriormente ser utilizado para outras funções. Contudo, se esse equipamento fosse excluído completamente, seria feita uma substituição do disco interno e realizada uma declaração de venda para o posterior responsável.
	11.2.8	Equipamento de utilizador autónomo	Verificar se os utilizadores garantem que o equipamento não assistido tenha proteção.	Os utilizadores não têm acesso aos servidores, no entanto apenas alguém que se equipare ao mesmo

				nível de cargo do administrador, tem acesso a esses equipamentos protegidos.
	11.2.9	Política de mesa clara e tela clara	Verificar: - Se existe um arquivamento de documentos e mídias de armazenamento removível; - Se existe adoção do *"clear screen"* para instalações de processamento de informações.	Não era possível o armazenamento removível pois era definido em todos os equipamentos através da BIOS, o desativamento de discos amovíveis. No entanto. A informação era toda realizada digitalmente, não havendo arquivos e papéis em cima de qualquer suporte, exceto programadores que queiram desenvolver esboços num papel (ex. estruturas de árvores ou realização de código), no entanto os esboços ficariam dentro da empresa para posteriormente serem eliminados com segurança. Nas máquinas (demonstrado o do administrador), existe a adoção diminutiva de pastas no seu ecrã de computador, chamado de "ecrã limpo/clear screen", não havendo a opção de saberem que documentos confidenciais estão em acesso no ambiente de trabalho.
Segurança nas operações				
A.12	12.1	Procedimentos e responsabilidades operativas		
	12.1.1	Procedimentos operativos documentados	Verificar se os procedimentos operativos foram documentados e disponibilizados a todos os utilizadores que precisam deles.	Sem observações.
	12.1.2	Gestão de alterações	Verificar se foram controladas as alterações na organização, processos de negócios, processamento de informações, instalações e sistemas que afetam a segurança da informação.	Obs.: Em termos de servidores haviam alertas. A gestão de alterações era realizada pelo administrador, no entanto, não está documentado.

	12.1.3	Gestão de capacidade	Verificar se os usos de recursos foram monitorizados, ajustados e projetados requisitos de capacidade futura para garantir o desempenho do sistema.	Sem observações.
	12.1.4	Separação de ambientes de desenvolvimento, teste e operativos	Verificar se o desenvolvimento e teste foram separados para reduzir os riscos de acesso não autorizado ou alterações nos sistemas operativos.	Sem observações.
	12.2	Proteção contra *malware*		
	12.2.1	Controlos contra *malware*	Verificar se estão implementados os controlos de deteção, prevenção e recuperação para proteção contra *malware*.	Implementada proteção contra antivírus. Implantação de softwares: Linux- ClamAV ou Clam Antivírus; Windows- McAfee.
	12.3	*Backup*		
	12.3.1	Backup de informações	Verificar se existe um processo para assegurar que as cópias de segurança de informação, software e imagens do sistema foram executadas e testadas regularmente de acordo com a política de backup?	Não há política, mas há backups, afirmando não sendo fáceis de gerir. Os backups de documentação digital funcionam através do **ownCloud** (gratuito). Desvantagem: Não são realizadas cópias de máquinas virtuais, ou seja poderão haver perdas de informação.
	12.4	*Login* e Monitorização		
	12.4.1	Registo de eventos	Verificar se existem registos de auditoria das atividades de utilizadores, exceções, eventos de segurança da informação, falhas e informações de utilizadores.	Eventos como a firewall, ou ver eventos dos servidores, são verificados 1x por semana. Função realizada apenas pelo Administrador da empresa.
	12.4.2	Proteção de informações de log	As informações e sistemas de log protegidos estão protegidos contra falsificação e acesso não autorizado?	Obs.: Os servidores fazem a criação de *logs* e o administrador aceita.

	12.4.3	*Logs* de administrador e operador	Verificar se as atividades de administrador e operador do sistema estão registados e os *logs* protegidos e atualizados.	Obs.: Não existe operador, apenas administrador.
	12.4.4	Sincronização do relógio	Verificar se os relógios de todos os sistemas de informação relevantes, dentro de uma organização ou domínio de segurança estão sincronizados com uma fonte de tempo precisa.	Nos sistemas operativos *Linux* e Windows é possível a sincronização interna e externa. Por exemplo, nas emissões de certificação é obrigatório a sua utilização.
	12.5	Controlo de *software* operativo		
	12.5.1	Instalação de software em sistemas de produção	Verificar se existem procedimentos para controlar a instalação do software nos sistemas de produção.	Obs.: Referente apenas à instalação de software nos servidores em produção. Nos servidores apenas são realizados updates de segurança e de instabilidade.
	12.6	Gestão de vulnerabilidades técnicas		
	12.6.1	Gestão de vulnerabilidades técnicas	Verificar se existem informações sobre vulnerabilidades técnicas de sistemas de informação, apropriadas para abordar o risco associado.	Sem observações.
	12.6.2	Restrições na instalação do software	Verificar se as regras que regem a instalação do software pelos utilizadores estão implementadas.	Por norma, podem instalar o que quiserem, normalmente é o spotify. Caso os utilizadores instalem um torrent, é controlado pela demora na linha.
	12.7	Considerações sobre auditoria de sistemas de informação		
	12.7.1	Controlos de auditoria de sistemas de informação	Verificar se os requisitos e atividades de auditoria que envolvam a verificação nos sistemas de produção devem ser planeados e acordados para minimizar as interrupções nos processos de negócios.	Consultou-se as diretrizes correspondentes ao mesmo ponto na norma 27002:2013. Sem observações.
Segurança nas Comunicações				

A.13	13.1	Gestão na segurança das redes		
	13.1.1	Controlos de rede	Verificar se as redes foram geridas e controladas, com o intuito de proteger (ameaças) as informações em sistemas e aplicações que utilizem a rede.	Obs.: *MAC Address*, *Firewalls*, *Routers* e autenticações.
	13.1.2	Segurança de serviços de rede	Verificar: - Se existem mecanismos de segurança, níveis de serviço e requisitos de gestão de todos os serviços de rede; - Se foram identificados e incluídos acordos de serviços de rede; - Se esses serviços são fornecidos internamente ou terceirizados.	Todos os serviços internos que a empresa tem em sua posse, só são acedidos por autenticação e maior parte dos funcionários não têm essa autenticação.
	13.1.3	Segregação em redes	Verificar se grupos de serviços de informação, utilizadores e sistemas de informação foram separados em redes.	Existe a segregação em redes, como por acessos *wireless*, *VPN* e *LAN* (interna).
	13.2	Transferência de informação		
	13.2.1	Políticas e procedimentos de transferência de informações	Verificar se existem procedimentos e controlos formais de transferência, para proteção da transferência de informações, através da utilização de todos os tipos de meios de comunicação.	Não aplicável; Sem observações.
	13.2.2	Acordos sobre transferência de informações	Verificar se foram adotados acordos para a transferência segura de informações comerciais entre a organização e as partes externas.	"Se não há uma transferência de informação, como é possível a existência de acordos da transferência de informação?" Obs.: Mesmo que não se aplique, é feita uma "transferência de comunicação" no local.

	13.2.3	Mensagens eletrónicas	Verificar se as informações envolvidas nas mensagens eletrónicas estão devidamente protegidas.	É protegido através da assinatura digital, no qual se sabe que aquele email é o original. As mensagens não são encriptadas, porque por mais que o emissor tenha facilidade, não teria a certeza se o recetor da mensagem recebeu a chave para desencriptar ou se seria do seu conhecimento saber fazer os posteriores procedimentos.
	13.2.4	Acordos de confidencialidade ou não divulgação	Verificar se existem requisitos para acordos de confidencialidade ou não divulgação, refletindo as necessidades da organização para a proteção de informações.	Existem acordos de confidencialidade e de não divulgação. A tarefa é realizada sempre de empresa para empresa, e na IL, o cargo de atuação pertence apenas ao administrador.
Aquisição, Desenvolvimento e Manutenção de Sistemas				
A.14	14.1	Requisitos de segurança dos sistemas de informação		
	14.1.1	Análise e especificação de requisitos de segurança da informação	Verificar se os requisitos relacionados com a segurança da informação estão incluídos nos requisitos para novos sistemas de informação ou aprimoramentos nos sistemas de informação existentes.	Todos os requisitos implementados nos sistemas de informação têm de evoluir conforme os sistemas de informação, desta forma, todos os requisitos anteriores precisam de ser atualizados e possivelmente eliminados.
	14.1.2	Proteger serviços de aplicativos em redes públicas	Verificar se as informações envolvidas nos serviços de aplicativos que passam por redes públicas estão contra atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas.	Utilização de encriptação local e a existência de firewall. De acordo com o **ODOO** as informações nos serviços, passam por redes públicas. As atividades fraudulentas e as disputas contratuais são verificadas e analisadas.
	14.1.3	Proteger transações de serviços de aplicativos	Verificar se as informações envolvidas nas transações de serviços de aplicativos foram protegidas para evitar a transmissão incompleta, navegação incorreta, alteração, divulgação, duplicação não autorizada de mensagens.	Obs.: Respetivo a entidades que fazem transações e microtransações. Obs.: Se for uma aplicação de desenvolvimento próprio, é necessário ter um sistema que envie e receba uma notificação de aviso "entregue" (não

				acontece com o email). Se for na receção de mensagens, é só necessário informar que o recetor leu e recebeu.
	14.2	Segurança nos processos de suporte e desenvolvimento		
	14.2.1	Política de desenvolvimento seguro	Verificar se as regras para o desenvolvimento de *software* e sistemas foram estabelecidas e aplicadas aos desenvolvimentos dentro da organização.	Sem observações.
	14.2.2	Procedimentos de controle de alterações do sistema	Verificar se as alterações nos sistemas do ciclo de vida de desenvolvimento foram controladas pelo uso de procedimentos formais de controlo de alterações.	Adaptação de versões. Vê-se as aplicações 1x a cada 3 meses, consultando sempre o mercado para ver aplicações que possa favorecer a empresa.
	14.2.3	Revisão técnica de aplicativos após alterações na plataforma operativa	Verificar: - Se as plataformas operativas foram alteradas; - Se os aplicativos críticos para os negócios foram revistos e testados para garantir que não haja impacto adverso nas operações ou na segurança organizacional.	Sempre que se realiza updates aos servidores, são testadas as aplicações para ver o seu funcionamento. Sempre que existe um update de um SO, o impacto pode ser significativo.
	14.2.4	Restrições sobre mudanças nos pacotes de software	Verificar se as modificações nos pacotes de *software* foram limitadas a mudanças necessárias e todas as mudanças devem ser rigorosamente controladas.	São feitos updates, pacotes de segurança, pacotes que têm impacto no Sistema operativo. A "**.NET**" é um exemplo na mudança de versões, que atualmente prejudica o funcionamento nas máquinas, devido ás suas alterações.
	14.2.5	Princípios de engenharia de sistemas seguros	Verificar se os princípios para engenharia de sistemas seguros estão estabelecidos, documentados, mantidos e aplicados a quaisquer esforços de implementação nos sistemas de informação.	(Verificar com o Artigo 25.º do RGPD). Obs.: Não é obrigatório construir de raiz a parte da segurança. Porém, posteriormente pode-se implementar medidas como a pseudonimização e encriptação.

	14.2.6	Ambiente de desenvolvimento seguro	Verificar se a organização estabelece e protege adequadamente a segurança do ambiente de desenvolvimento e integração de sistemas, que cobrem todo o ciclo de vida do desenvolvimento do sistema.	Obs.: Existe, é mantido e atualizado.
	14.2.7	Desenvolvimento terceirizado	Verificar se a organização supervisiona e monitoriza as atividades de desenvolvimento de sistemas terceirizados.	Não aplicável; Sem observações.
	14.2.8	Teste de segurança do sistema	Verificar se o teste da funcionalidade de segurança é realizado durante o desenvolvimento.	Os testes de funcionalidade são realizados com várias fases. Primeira fase: Direcionam os testes para o Departamento de **Desenvolvimento;** Segunda fase: Redirecionam a alguém que tenha conhecimento da matéria, neste caso, o Administrador; Terceira fase: Redirecionam a pessoas que nada têm haver com a matéria de voto, para possíveis testes de erros, cognição e funcionalidade.
	14.2.9	Teste de aceitação do sistema	Verificar se os programas de teste de aceitação e critérios relacionados estão estabelecidos para novos sistemas de informação, atualizações e novas versões.	De acordo com o ponto anterior, caso cheguem ao fim da terceira fase, os mesmos são aceites.
	14.3	Dados de teste		
	14.3.1	Proteção de dados de teste	Verificar se os dados de teste são selecionados cuidadosamente, protegidos e controlados.	Não é aplicável. Obs.: Nunca são utilizados dados de clientes para a realização de testes.
Relações com Fornecedores				
A.15	15.1	Segurança da informação nos relacionamentos com fornecedores		

	15.1.1	Política de segurança da informação para relacionamentos com fornecedores	Verificar se os requisitos de segurança da informação para atenuar os riscos, (associados ao acesso do fornecedor aos ativos da organização) foram acordados com o fornecedor e documentados.	Não há política, pela razão que não há uso frequente de fornecedores. No entanto, existe uma política interna que informa o que fazer, o que dar e o que receber dos fornecedores. Porém, não existe uma política exterior de comunicação.
	15.1.2	Abordar a segurança nos contratos com fornecedores	Verificar se todos os requisitos de segurança da informação estão estabelecidos e acordados com cada fornecedor, para que se possa aceder, processar, armazenar, comunicar ou fornecer componentes da infraestrutura de TI para as informações da organização.	Sem observações.
	15.1.3	Cadeia de suprimentos de tecnologia da informação e comunicação	Verificar se os acordos com fornecedores incluem requisitos para tratar dos riscos de segurança da informação, associados aos serviços de tecnologia da informação, comunicação e produtos.	Equipamento que se pede para as instalações. Caso haja uma mudança de servidores, será necessário ter em conta de quem vai vender se tem capacidade para entregar o material, quanto tempo demora a entrega do material, de quanto em quanto tempo será necessário as manutenções e os **NDA'S**.
	15.2	Gestão da entrega de serviços a fornecedores		
	15.2.1	Monitorização e revisão de serviços de fornecedores	Verificar se a organização monitoriza, revista e audita regularmente a prestação de serviços do fornecedor.	(Ver a norma 9001:2015, relativamente ao ponto 7.5 "Informação documentada" (página 19) - avaliação de fornecedores). Obs.: Na IL existem fornecedores, nomeadamente a nível de equipamentos eletrónicos, exclusivamente a nível de hardware.

	15.2.2	Gestão de alterações nos serviços do fornecedor	Verificar se as mudanças na prestação de serviços pelos fornecedores, incluindo a manutenção e melhoria das políticas, procedimentos e controlos de segurança da informação existentes, foram geridas, levando em consideração a criticidade das informações, sistemas, processos de negócios envolvidos e a reavaliação dos riscos.	Seria interessante adotar esta política no que toca aos fornecedores de outsourcing. Implica a que maneiras e formas de trabalho sejam alteradas, ao invés do cliente comprar e o fornecedor diretamente entregar ao cliente, este abdica dos serviços usuais e fornece ao cliente serviços melhores e diferentes.
Gestão de Incidentes na Segurança da Informação				
A.16	16.1	Gestão de incidentes e melhorias na segurança da informação		
	16.1.1	Responsabilidades e procedimentos	Verificar se as responsabilidades e procedimentos de gestão foram estabelecidos, para garantir uma resposta rápida, eficaz e ordenada aos incidentes de segurança da informação.	Sem observações.
	16.1.2	Reportar eventos de segurança da informação	Verificar se os eventos de segurança da informação são relatados através dos canais de gestão apropriados, o mais rápido possível.	Obs.: Relatados ao administrador (Administração).
	16.1.3	Reportar falhas de segurança da informação	Verificar se os funcionários e contratados que usam os sistemas e serviços de informação da organização observam e relatam quaisquer deficiências observadas ou suspeitas de segurança das informações nos sistemas ou serviços.	Normalmente os incidentes são transmitidos à administração e tratamos no momento. Quanto aos eventos, não são prioritários, são analisados e tratados posteriormente.
	16.1.4	Avaliação e decisão sobre eventos de segurança da informação	Verificar se os eventos de segurança da informação são avaliados e decididos se devem ser classificados como incidentes de segurança da informação.	Se forem incidentes são momentaneamente corrigidos. Caso sejam eventos são posteriormente analisados. (relacionado com o ponto acima)

	16.1.5	Resposta a incidentes de segurança da informação	Verificar se os incidentes de segurança da informação são respondidos de acordo com os procedimentos documentados.	Primeiramente, os eventos são erros iniciais. Os incidentes categorizam-se como eventos posteriores nos quais as correções não foram priorizadas. No entanto, os eventos e incidentes têm de ser padronizados e categorizados de acordo com o seu nível de vulnerabilidades.
	16.1.6	Aprender com incidentes de segurança da informação	Verificar se o conhecimento adquirido com a análise e resolução de incidentes de segurança da informação, são usados para reduzir a probabilidade ou o impacto de incidentes futuros.	Relativamente à resolução de incidentes e eventos, se o erro voltar a acontecer então a resolução não foi a mais adequada para a resolução do incidente.
	16.1.7	Recolha de evidências	Verificar se a organização define e aplica procedimentos para a identificação, recolha, aquisição e preservação de informações, que podem servir como evidência.	Com as evidências descritas, realiza-se posteriormente um processo de auditoria que descreve todo o processo das evidências do ponto 16.1.6.
Aspetos de Segurança da Informação na Gestão da Continuidade de Negócios				
A.17	17.1	Continuidade da segurança da informação		
	17.1.1	Planeamento da continuidade da segurança da informação	Verificar se a organização determina requisitos de segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, como por exemplo durante uma crise ou desastre.	A IL não permite aos funcionários aceder ás instalações através de VPN's em outros locais, devido a múltiplos problemas de privacidade (ex. terrorismo e desastres físicos). Porém, existem repositórios em que ambos podem ser acedidos remotamente, e na IL existem duas vertentes de backup de informação: Documentos no **ownCloud** (equiparado à dropbox), e **openKM** (gestão documental). A nível de eficácia a ownCloud é maior e mais complexo e completo a nível de permissões. Estes locais remotos poderão ser acedidos através do início de sessão de utilizador.

	17.1.2	Implementação da continuidade da segurança da informação	Verificar se a organização estabelece, documenta, implementa e mantém processos, procedimentos e controlos para garantir o nível de continuidade necessário para a segurança da informação durante uma situação adversa.	Obs.: Está previsto ser futuramente implantado, no entanto, é um serviço dispendioso. Seria necessário atualizar anualmente.
	17.1.3	Verificar, revisar e avaliar a continuidade da segurança da informação	Verificar se a organização adquire os controlos de continuidade de segurança da informação estabelecidos e implementados em intervalos regulares, a fim de garantir que sejam válidos e eficazes em situações adversas.	(Consultar ponto acima). Sem observações.
	17.2	Redundâncias		
	17.2.1	Disponibilidade de instalações de processamento de informações	Verificar se as instalações de processamento de informações são implementadas com redundância suficiente para atender aos requisitos de disponibilidade.	Existem 4 domínios no VPS (servidores virtuais) ou duas transferências para servidores partilhados. O responsável refere que só é possível implementar uma VPS para o SO atualmente utilizado na empresa (Linux), tal como demonstrado no website Ptisp.pt.
Conformidade				
A.18	18.1	Cumprimento dos requisitos legais e contratuais (leis e contratos de lei)		
	18.1.1	Identificação da legislação aplicável e requisitos contratuais	Verificar se todos os requisitos estatutários, regulamentares, contratuais e legislativos relevantes e a abordagem da organização para atender a esses requisitos são explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação e organização.	Contratos com colaboradores (incluindo o outsourcing), fornecedores, e clientes. Vantajoso e utilizado para poder dar o conhecimento correto de como os fornecedores devem estabelecer as suas tarefas com todos os elementos da empresa. Provocando deste modo um fluxo de saída de informações que ocorrem por vínculos externos com a corporação, dentro da estrutura das economias nacionais e internacionais.

	18.1.2	Direito de propriedade intelectual	Verificar se foram implantados procedimentos, para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados aos direitos de propriedade intelectual e ao uso de produtos de software proprietários.	De acordo com o responsável, existem duas maneiras de averiguar a situação. Caso o ponto 18.1.1. esteja concluído, o ponto 18.1.2 encontra-se em também realizado, atualizado e em conformidade. Contudo, em relação aos direitos de propriedade intelectual, futuramente a IL pensará em adotar domínios para o sistema operativo Linux que controlem a eliminação da informação e códigos fonte apenas com a permissão do administrador. Relativo ao uso de produtos de software do Administrador: Windows, Office e Visual Studio 2019. No caso dos funcionários usam o Windows e o Community Edition Visual Studio, eliminado a opção de usar o Office.
	18.1.3	Proteção de registos	Verificar se os registos são protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos legislativos, regulamentares, contratuais e comerciais.	Sem observações.
	18.1.4	Privacidade e proteção de informações de identificação pessoal	Verificar se a privacidade e a proteção das informações de identificação pessoal, são garantidas conforme exigido na legislação e regulamentação relevantes, quando aplicável.	Sem observações.
	18.1.5	Regulação dos controles criptográficos	Verificar se os controlos criptográficos são utilizados em conformidade com todos os acordos, leis e regulamentos relevantes.	Não aplicável; Não IL não há desenvolvimento para entidades públicas.
	18.2	Revisões de segurança da informação		

	18.2.1	Revisão independente da segurança da informação	Verificar se a abordagem da organização para gerir a segurança da informação e a sua implementação (ou seja, objetivos, políticas, processos e procedimentos de controlo da segurança da informação) são revistas, independentemente em intervalos planeados ou quando ocorrem alterações significativas.	Obs.: Necessário a auditoria de um auditor externo. Este auditor, conhecido como um "revisor independente", que não pode pertencer à empresa, não pode ter nenhum conhecimento da organização em questão, incluindo o seu funcionamento. Tem a função de averiguar se o sistema está em conformidade com aquilo que foi especificado. De acordo com a norma 27002:2013, em consulta com o ponto referente ao 18.2.1 "*Independent review of information security*" (página 77), menciona exemplos de cargos e funções representáveis neste campo.
	18.2.2	Conformidade com políticas e normas de segurança	Verificar se os gerentes revisam regularmente a conformidade do processamento e dos procedimentos de informações na sua área de responsabilidade com as políticas, padrões e quaisquer outros requisitos de segurança adequados.	Obs.: Não necessária uma política que concretize este efeito. O requisito tem de estar de acordo com as vertentes abrangidas no ponto 5.3 "*Organizational roles, responsibilities and authorities*" (página 03), da norma 27001:2013, que refere as responsabilidades e funções organizacionais.
	18.2.3	Revisão da conformidade técnica	Verificar se os sistemas de informação são revisados regularmente quanto à conformidade com as políticas e padrões de segurança da informação da organização.	Necessário um revisor técnico. Ou então optar por o software Osint, Owasp, ou o OpenVAS (greenbone). Normalmente são software gratuitos, no entanto a eficácia de um "report" dado como resultado destes softwares não é tão eficaz como a análise realizada por um especialista técnico.

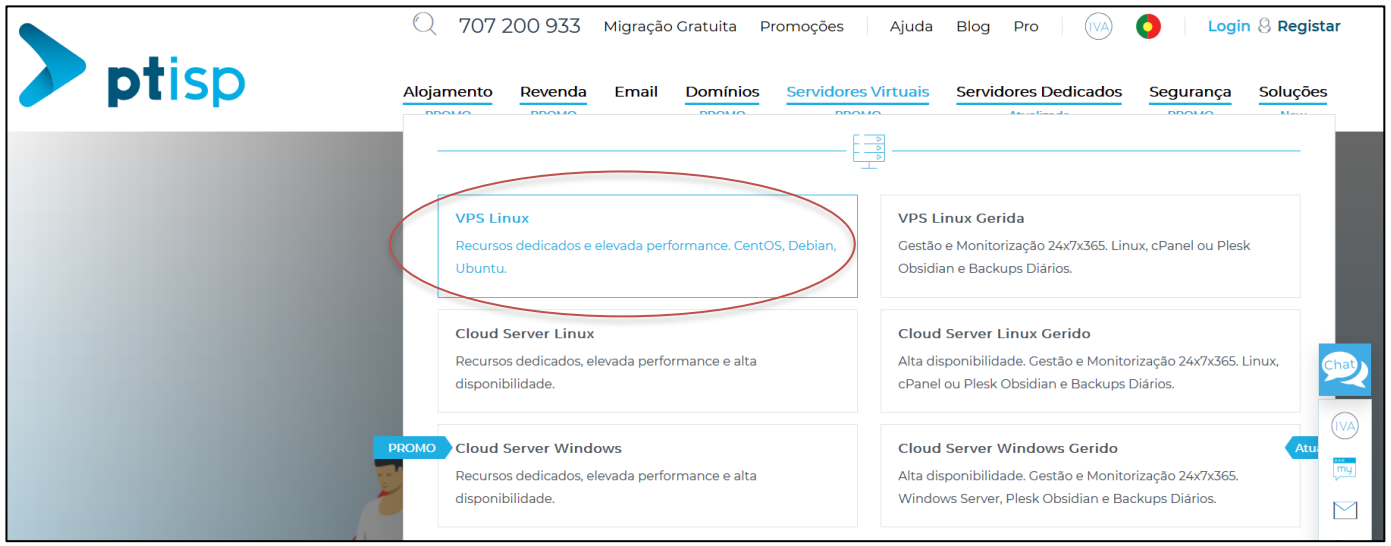


Figura 18 - Servidores Virtuais

* Imagem referenciada ao ponto 17.2.1

Manual

de

Boas Práticas

ORG. INTERACTION LAYER

(Segurança da Informação)

Porto - julho 2020

Manual de Boas Práticas

INTERACTION LAYER

Endereço: Praça de Mouzinho de Albuquerque, 113, 4100-359, Porto

Créditos: Elaborado por Susana Filipa Silva Cardoso Dias

Resumo:

Os estabelecimentos que atuam na área da Informática, estão frequentemente envolvidos em furtos, ameaças e riscos baseados na Segurança da Informação.

Torna-se assim necessário implementar as Boas Práticas da segurança da informação, respetivamente associada à norma ISO/IEC 27001:2013 com o intuito de aumentar a segurança e a qualidade da empresa, proporcionando uma melhor satisfação por parte dos colaboradores e confidencialidade para com o cliente.

Sumário

Definições, siglas e abreviaturas

Browser – (Navegador Internet), é um programa criado para permitir a navegação pela internet. É o que torna possível aceder a sites (ex. Firefox, Google Chrome, Internet Explorer).

Clean desk – (Política de Mesa Limpa), pontifica que todos os colaboradores devem limpar as suas mesas no final de cada dia de trabalho, como documentos, post-its, e dispositivos removíveis (ex. cartões de memória USB). Esta política ajuda na organização a reduz o risco de roubo de informações, fraude ou violação de segurança causada por informações confidenciais deixadas sem supervisão e visíveis à vista.

Clouds – ("*Cloud Computing Services"*), utilizada no armazenamento de dados e recursos do sistema, sem a gestão ativa-direta do utilizador.

CNCS - Centro Nacional de Cibercegurança (Portugal).

Firewall - Dispositivo de uma rede de computadores, na forma de um programa, que tem por objetivo aplicar uma política de segurança, normalmente associado a redes.

UPS - ("*Uninterruptible Power Supply"*), é um aparelho elétrico que fornece energia de emergência quando a fonte de energia de entrada ou a energia da rede elétrica falha.

No-break - Sistema de energia auxiliar ou de emergência ou um indutor de reserva, fornece proteção quase contra interrupções de energia de entrada, fornecendo energia armazenada em baterias. É um tipo de sistema de energia contínuo.

ID - ("*Identifier"*), é um nome que identifica ou rotula a identidade de algo. Pode ser uma palavra, número, letra, símbolo ou uma combinação dos anteriores.

PIN – ("*Personal Identification Number"*) é o nome frequente utilizado para definir senhas de pelo menos quatro caracteres usadas em cartões SIM, dispositivos móveis, cartões de crédito e outras aplicações.

(Cartão) ***SIM*** – Definido como um cartão inteligente utilizado para identificar e armazenar dados de dispositivos móveis.

Software - Sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. Também pode ser definido como programas que comandam o funcionamento de um computador (aplicativos computacionais).

URL – ("*Uniform Resource Locator"*), refere-se a um endereço de rede no qual se encontra algum recurso informático (ex. arquivo de computador) ou um dispositivo periférico (ex. impressora, unidade de rede). Porém, essa rede pode ser a Internet.

1. Introdução à Segurança de Informação

No presente capítulo serão apresentados conceitos relativos à segurança de informação, com questões relacionadas com a importância da sua implementação em serviços e empresas.

Temática abordada:

Na era em que as informações eram armazenadas apenas em suporte de papel, a segurança era relativamente simples. Bastava arquivar os documentos num lugar seguro, de modo a restringir o acesso físico a qualquer entidade exterior. Devido às mudanças tecnológicas e ao uso de computadores de grande dimensão, a estruturação da segurança ficou mais sofisticada, com implementação de controlos lógicos centralizados. No entanto, com a chegada da época dos "*personal computers*" e da gênese das redes de computadores, as quais se conectam no mundo inteiro, onde os aspetos de segurança atingiram uma gigantesca complexidade, atualmente cada vez mais sofisticados. Simultaneamente, os sistemas de informação adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que, sem os conteúdos materiais como computadores e redes de comunicação, a prestação de serviços tornar-se-ia impraticável.

1.1. A quem se dirige o documento?

Apresenta-se por meio de capítulos, um guia de boas práticas correlacionadas com a segurança da informação. Dedicado a qualquer colaborador pertencente à empresa *Interaction Layer,* que interaja de alguma forma com ambientes informatizados até profissionais das tecnologias de informação, que envolvam relações com conteúdos da segurança de informação. Com a finalidade de poder vir a proteger a organização, conservar a privacidade e os seus recursos herdantes, investimentos e negócio.

1.2. O que significa "Segurança da Informação"?

Tópicos como a Segurança da Informação estão diretamente relacionados com a proteção de um conjunto de informações, no sentido de vir a preservar o valor que possuem para uma empresa. Tencionam garantir principalmente questões relacionadas com a integridade, confidencialidade, autenticidade e disponibilidade das

informações processadas por uma dada organização.

1.3. Quem é responsável pela segurança da informação de uma empresa?

Todos os colaboradores são responsáveis pela segurança da informação da empresa e cada um tem a responsabilidade de proteger os seus dados e os que nos são confiados.

1.4. Princípios gerais da segurança da informação de uma empresa

A proteção eficaz e adequada da informação e dos sistemas de informação contra quebras de confidencialidade, de integridade e de disponibilidade garante a capacidade de produção e a posição concorrencial da organização, a confiança junto dos clientes e parceiros, bem como a imagem junto do público, faz parte imprescindível da política da organização.

- Reagimos de imediato e adequadamente à situação em caso de violação da segurança;
- Garantimos a disponibilidade dos sistemas de informação com base nas exigências dos processos de negócio;
- Implementamos procedimentos adequados à não interrupção da atividade;
- As regras de segurança da informação são afixadas e comunicadas aos colaboradores, fornecedores e parceiros.
- Estamos cientes da elevada importância da segurança da informação para a nossa organização e tratamo-la de forma adequada;
- Implementamos procedimentos sistemáticos que visam a redução dos riscos;
- Incutimos a responsabilidade pela segurança da informação;
- Estabelecemos medidas adequadas à nossa organização para garantir a segurança da informação. Verificamos regularmente o respetivo cumprimento e a eficácia;
- Protegemos a informação própria e a que nos é confiada, impedindo a sua divulgação e alteração ilegal.

2. Proteção de recursos e controlos de Informação

No presente capítulo, serão apresentados conceitos fulcrais sobre a importância da implantação de controlos de acesso na empresa e os recursos dos quais à priori devem ser protegidos. A finalidade baseia-se em demonstrar como um utilizador se pode proteger com segurança quando acede a recursos e informações.

Temática abordada:

Os controlos de acesso, têm objetivos que se relacionam com a proteção de equipamentos, aplicativos e arquivos de dados contra perdas, modificações ou possivelmente a divulgação não-autorizada. A tecnologia computacional difere bastante em relação a outros tipos de recursos, onde os mesmos não poderão ser facilmente protegidos com dispositivos físicos (ex. alarmes, cadeados).

Este capítulo mostra motivos pelos quais estes recursos devem ser protegidos.

2.1. Proteção de recursos

- Programas fonte de código

Um dos principais riscos que uma empresa que atua no setor informático é o acesso não-autorizado ao código fonte dos programas, além de poder ser usado para realizar alterações às funções lógicas do programa.

- Arquivamento de dados

Conteúdos como bases de dados, arquivos ou transações bancárias, devem ser devidamente protegidas para evitar que os mesmos sejam modificados ou eliminados sem autorização (ex. arquivos com a configuração do sistema, recibos de pagamentos, dados estratégicos da empresa).

- *Softwares* e dispositivos eletrónicos

O acesso a softwares (ex. editores, compiladores, aplicações de monitorização e de diagnóstico) devem ser restritos, já que são ferramentas que poderão vir ajudar na alteração de aplicativos, arquivos de dados e configurações a nível de dispositivos eletrônicos. Esses dispositivos, pertencentes à empresa, como computadores, são um alvo bastante pretendido, pois o "todo" da fragilidade é a sua configuração. Comprometendo assim, a segurança de toda a informação adicional.

- Arquivo de palavras-passe (*passwords*)

A falta adequada na proteção de arquivos que armazenam as senhas, é um risco elevado no qual se pode comprometer todo o sistema, já que basta uma entidade não-autorizada, que obtenha o ID e senha do mesmo, e, intencionalmente, causar estragos ao sistema.

Convém sempre manter a *password* segura e secreta, podendo assim evitar que alguém (com intenções maliciosas), consiga aceder às plataformas que estão protegidas por passwords (ex. email, *clouds*, redes sociais).

- Arquivo de inícios de sessão (*logins*)

Usados para registar os movimentos dos utilizadores, são ótimos para análise de posteriores auditorias. Os logins registam quem acedeu aos recursos computacionais, aplicativos, arquivos de dados e softwares, quando se fez o acesso e que tipo de ações foram efetuadas.

2.2. Recomendações e constituição de uma palavra-passe (*Passwords*)

- Não guardar a password em listas ou browsers;
- Constituição (segundo a CNCS):
  - Utilizar mais de 10 caracteres;
  - Utilizar letras maiúsculas (A...Z);
  - Utilizar letras minúsculas (a...z);
  - Utilizar algarismos (0...9);
  - Utilizar caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /);
  - Utilizar em alternativa, frases ou excertos de texto longo conhecidos pelo utilizador, sem o caracter «espaço»;
  - Evitar o uso de termos previsíveis e dados de informações pessoas (ex. nome, cidade, ano nascimento, *qwerty*);
  - Alterar a *password* de origem na compra de um equipamento ou dispositivo;
  - Alterar a *password* regularmente, mesmo que os sistemas não te obriguem a fazê-lo (correto seria de 2 em 2 meses);
  - Memorizar as *passwords* em vez de as registar em papel ou digitalmente, ou em locais visíveis;
  - Se possível, implementar uma autenticação de duplo fator;
  - Usar uma password diferente em cada sistema da organização e sistemas pessoais (email, redes sociais, aplicações de *softwares*).

3. Segurança e controlos de acesso física

No terceiro capítulo, serão apresentados controlos de acesso físico e a sua importância de implementação na empresa. Salvaguardar esta categoria de segurança, aumenta a proteção física como a proteção dos sistemas de informação.

Temática abordada:

A segurança física é um dos passos fundamentais que se deve dar em primeiros. A mesma corresponde à possível constituição de "barreiras" de forma a evitar intrusões, garantindo desta forma uma resposta eficiente às mesmas. Esta categoria de segurança, previne acessos não-autorizados a equipamentos, instalações, materiais ou documentos.

3.1. Recomendações de controlo de acesso físico?

- Controlar a entrada de pessoas numa área de segurança para que apenas pessoas autorizadas tenham acesso.
- Registar a hora e data de entrada de cada entidade exterior à empresa;
- Permissões de acesso à área deve ser realizada apenas para finalidades autorizadas;
- As áreas como salas de servidores, devem ser restritas às pessoas exteriores;
- A todos os colaboradores e terceiros será necessária uma identificação visível à entrada (ex. cartão de identificação).

3.2. Recomendações de infraestruturas de utilidades?

- Exigir manutenções regulares em infraestruturas no tratamento de esgotos, abastecimento de água, energia elétrica e ar-condicionado;
- Adotar um sistema *UPS* (*Uninterruptible Power Source*). Recomenda-se o *No-break;*
- Implementar um indutor de emergência caso haja alguma complicação na empresa.
- Implementar um circuito fechado de vigilância constante sobre os pontos críticos da empresa.
- Os conteúdos das filmagens devem ter um controlo rígido de acesso.

3.3. Recomendações segurança física de equipamentos

- Implementação de controlos contra sabotagens e furtos;
- Inibição de bebidas ou comidas próximas de equipamentos;
- Optar pelo uso de cabos de segurança para computadores e tablets;
- A posição do monitor do computador, deve de alguma maneira estar a evitar a sua visualização de informações para outras pessoas;
- Analisar regularmente as condições ambientais (humidade, poeira e a temperatura de todos os dispositivos eletrónicos);
- Desligar da fonte de energia equipamentos que não necessitem de ficar ligados;
- Evitar o armazenamento de dados em pastas locais;
- Documentos de trabalho devem estar armazenados nas pastas de rede;
- Permitir apenas o uso de dispositivos e equipamentos autorizados;
- Ativar o bloqueio automático em todos os equipamentos tecnológicos, sendo vital e será a cuidado e responsabilidade de cada colaborador não deixar os mesmos desbloqueados (+ L);
- Utilizar *PINs* e *passwords* de acesso com limite de tentativas de acesso;
- Desativar ou proteger a câmara de cada computador na empresa e ativar assim que for necessário;
- Utilizar filtros de privacidade nos computadores da empresa.

3.4. Recomendações segurança contra desastres físicos

- Precauções contra incêndios.
  - Formação de plano de treino contra incêndios;
  - Evitar que equipamentos inativos por utilizadores estejam ligados;
  - Evitar qualquer atividade que provoque fumo, ou libertação de gás em qualquer instalação;
  - Implementar extintores e caso haja uma sede exterior uma boca de incêndio;
  - Evitar qualquer atividade que provoque fumo, ou libertação de gás em qualquer instalação;

- Antes da saída de qualquer colaborador da empresa devem:
  - Verificar se o sistema de emergência e prevenção de falhas está ativo;
  - Qualquer conteúdo físico (papel) deve ser recolhido e se assim que possível descartado.

4. Proteção e advertências em postos de trabalho e salas de reuniões

No capítulo 4, serão apresentados controlos para proteção relativos aos postos de trabalho, e advertências da importância com recomendações nas salas de reuniões, para impossibilitar qualquer fuga de informação confidencial. Este capítulo remete à finalidade de implementação de medidas e procedimentos que protegem o teu posto de trabalho, a informação do negócio e os teus dados pessoais.
No mundo "internet" existem especificas regras e códigos de conduta, com o objetivo de melhorar a segurança da informação.

Temática abordada:

O posto de trabalho usufrui de ser uma ferramenta cuidadosamente pensada para que colaboradores possam trabalhar de forma confortável, organizada, adequada e confortável no encargo das suas funções.

É constituído por documentos que fazem parte de uma rede organizacional, incluída por computadores e outros equipamentos tecnológicos.

Por regra, todos os colaboradores da empresa fazem parte da cadeia de segurança.

4.1. Recomendações e advertências para postos de trabalho?

- O posto de trabalho deve estar sempre organizado e "*clean desk*";
- Durante reuniões, dedicada a temas sensíveis ou confidenciais, devem verificar se o local está corretamente protegido e fechado, para ser apenas partilhada de forma confidencial.
- No fim do dia, deve-se verificar se as janelas e portas ficaram corretamente fechadas.

4.2. Advertências de correio eletrónico (email)

- Boas Práticas de utilização do correio eletrónico.
  - Utilizar sempre o email de forma profissional;
  - Verificar sempre os endereços de email dos destinatários;
  - Inibir a abertura de emails de origem desconhecida; eliminar permanentemente;
  - Não enviar informação pessoal que seja solicitada por email (ex. n.º cartão crédito, password, email);

- Não abrir ligações de emails considerados suspeitos;
- Informações confidenciais (exceto *passwords*) ou dados possuais só podem ser enviados encriptados;

4.3. Recomendações da eliminação de dados e dispositivos de impressão

A eliminação de documentos que contêm informação confidencial, deve ser realizada de acordo com procedimentos adequados e regras especificas de segurança.

- Existir um contentor de eliminação de documentos de suporte de papel;
- Nesse contentor, junto deve haver uma pasta com formulário para registar o material colocado, a data e hora do mesmo;
- A eliminação de qualquer impressão deve ocorrer na instalação da empresa, e apenas realizada pelo administrador;
- Equipamentos eletrónicos só podem ser destruídos e/ou" apagados", apenas pelo administrador

4.4. Advertências de limites na navegação de Internet

Atualmente veio-se a distinguir que a comunicação e informação é considerada a "chave" do sucesso empresarial. Por esse mesmo motivo, é importante comunicarmos de forma segura, transmitindo apenas a informação necessária.

- Navegação da Internet.
  - Certificar se o site é seguro (analisar o "cadeado" ou aceder pelo endereço (URL) que deve começar por "https://" e não por http://);
  - Consultar extratos das contas bancárias e serviços com regularidade;
  - Certificar se o *browser* e o antivírus estão atualizados;
  - Usar uma *firewall* pessoal;
  - Inibir o acesso a sites com conteúdos ilegais ou inadequados;
  - Não é permitido na transferência de ficheiros e *clouds* a troca de dados pessoais da organização;
  - Inibir a divulgação de informação organizacional nas redes sociais;
  - Inibir a utilização de ferramentas da internet para criar ou traduzir conteúdos (ex. Google *Translate* ou *Prezi*);
  - Inibir ações de jogo online ou apostas com equipamentos/dispositivos da empresa (ex. Rede, Computadores, telemóveis).
  - Permitir o uso da aplicação "*Spotify*" (serviço de *streaming* de música).

5. Adoção de práticas remotas na organização

No presente capítulo, serão apresentados conceitos relativos à prática de métodos via teletrabalho, com questões relacionadas com a importância de como esta implementação concebe uma vasta procura em serviços e empresas.

Temática abordada:

Atualmente, o funcionamento das empresas encontra-se sucessivamente destacado nos sistemas informáticos, dado que a utilização da tecnologia tem vindo a alterar o modo como os contratados prestam a sua atividade de trabalho.

A influência da tecnologia é, pois, evidente e o "teletrabalho" é uma grande oportunidade para todos os setores da sociedade, principalmente quando estes passam por um risco de trabalho.

Considera-se "teletrabalho", a prestação laboral, exterior a qualquer instalação da empresa, através de recursos informáticos e de comunicação, cujo determinado no regime jurídico (Artigos n.º 165.º a 171.º)[1] do Código do Trabalho[2].

Porém, todo o trabalho remoto ou realizado à distância, abrange riscos para a segurança da informação da empresa, sendo relacionados com a utilização de dispositivos tecnológicos e/ou conectados à internet (ex. *Phishing* relacionado com a pandemia do Covid-19);

5.1. Quando deve a empresa recorrer a teletrabalho ou trabalho remoto?

Se o cargo do trabalhador for de alguma forma compatível com a adoção desse mesmo regime, e desde que o responsável da empresa possa assegurar ao trabalhador em questão os recursos necessários para o a ocorrência, tanto quanto possa suportar os custos associados a essa ocupação. Porém, será necessário fazer cumprir o alerta de que o regime de teletrabalho deverá submeter-se a uma formalização de regras pré estipuladas.

[1] Artigo 165.º - Noção de teletrabalho
Artigo 175.º - Admissibilidade de contrato de utilização de trabalho temporário

[2] (Lei n.º 93/2019, de 04/09)

5.2. Condições essenciais para quem realiza teletrabalho

- Utilizar apenas dispositivos autorizados pela empresa;
- Não partilhar estes dispositivos autorizados com amigos e familiares;
- Garantir com o Departamento Security da empresa, que os dispositivos estão atualizados e possuem um antivírus e a *firewall* ativos;
- Realizar *backups* regulares para *clouds* ou dispositivos externos;
- Evitar usar o serviço de Wi-Fi pertencente a espaços públicos;
- Utilizar sempre a VPN da empresa;
- Não abrir mensagens de correio eletrónico, mensagens de texto, ou nem premir links ou anexos de efeitos desconhecidos;
- Recusar a partilha de informação profissional nas redes sociais;
- Garantir que o Wi-Fi pessoal, tenha uma password forte e, se ainda não estabeleceu esse requisito, altere o mais cedo possível.

5.3. Quais seriam as alternativas da a realização de reuniões e a implementação de "*Webinars*"?

Primeiramente, "*Webinar*", significa efetuar uma conferência online (videoconferência), com intuito seja profissional, educacional ou académico, na qual remete apenas uma via para que o conferencista se expresse, onde diversamente outras pessoas assistem.

No entanto, a aplicação de reuniões e *webinars* via aplicação de comunicação "*ZOOM*", é cada vez mais adotada como ferramenta de trabalho à distância, seja entre clientes e colaboradores de uma organização. Com a finalidade de poder garantir aos utilizadores uma maior segurança na sua utilização, é aconselhável pela CNCS (CNCS, 2020) [3]

- ✓ Optar por restringir os eventos, apenas a utilizadores autenticados;
- ✓ Criar uma senha de acesso único para cada reunião efetuada;
- ✓ Ativar a criptografia ponto-aponto nas reuniões;
- ✓ Definir as permissões de gravação adequadas;
- ✓ Utilizar assinaturas de áudio;
- ✓ Utilizar marcas de água na partilha de ecrã.

[3] CNCS. (2020). Cibersegurança em reuniões online e webinars (p. 1). CNCS Portugal. https://www.cncs.gov.pt/content/files/ciberseguranca_em_reunies_online_e_webinars.pdf

Manual

de

Boas Práticas

ORG. INTERACTION LAYER

(Segurança da Informação)

Porto - julho 2020