Universidade do Minho
Escola de Engenharia

José Luís da Silva Alves

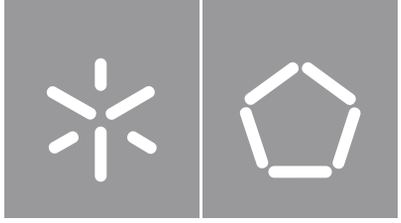
Roadmap **para a Segurança da Informação numa empresa de Logística**

junho de 2022

Roadmap **para a Segurança da Informação numa empresa de Logística**

José Luís da Silva Alves

UMinho | 2022



Universidade do Minho
Escola de Engenharia

José Luís da Silva Alves

Roadmap para a Segurança da Informação numa empresa de Logística

Dissertação de Mestrado
Mestrado Integrado em Engenharia e Gestão Industrial

Trabalho efetuado sob a orientação do
Professor Doutor Rui Manuel de Sá Pereira Lima
Professor Doutor Cristiano de Jesus

junho de 2022

AGRADECIMENTOS

Reservo aqui o espaço para agradecer a todos aqueles que, de alguma forma, direta ou indiretamente, me apoiaram e auxiliaram para a realização da minha dissertação de mestrado.

Aos meus orientadores, Professor Rui Lima e Professor Cristiano de Jesus, por terem aceitado o papel de me orientar, pelos ensinamentos, disponibilidade e respetiva ajuda no desenvolvimento deste projeto de dissertação.

Aos meus orientadores da empresa, Engenheiro Miguel Cordeiro e Engenheiro Luís Correia, por me terem acolhido no seu departamento, orientado e acompanhado ao longo de todo o projeto. Um especial obrigado à Doutora Catarina Azevedo, pela paciência e enorme disponibilidade para me ensinar todo o conteúdo que necessitara para o sucesso do projeto.

Também quero agradecer aos meus amigos pelo incentivo, todas as palavras de motivação e especialmente pelo contributo e presença ao longo dos cinco anos que frequentei a Universidade do Minho, tornando-os, assim, nos melhores anos da minha vida.

A todos os professores, tutores e conselheiros que fizeram parte, de algum modo, no meu percurso ao longo destes anos na universidade, pelo que a sua presença no meu percurso, tenha contribuído para minha conclusão vitoriosa neste ciclo.

Por fim, um especial agradecimento, aos meus pais, irmãs e restantes membros da família, pela tranquilidade, força e coragem transmitida, não só durante o período da dissertação e ensino superior, mas também por toda a educação que me transmitiram e que, consequentemente, contribui para o meu sucesso escolar e profissional.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

RESUMO

A presente dissertação foi elaborada no abito geral do grau de mestre em Engenharia e Gestão Industrial, com o intuito de descrever o projeto de investigação desenvolvido na *Rangel Logistics Solutions*. A dissertação intitula-se de "*Roadmap* para a segurança da informação numa empresa de Logística". Este projeto surgiu do facto da empresa, não só ambicionar a obtenção de uma certificação da norma internacional ISO 27001:2013, mas também melhorar o nível de maturidade de segurança das TI– objetivo principal desta dissertação - e consequentemente, obter uma conformidade total com o regulamento geral de proteção de dados.

A metodologia de investigação seguida foi "Investigação-Ação". Começando com uma revisão bibliográfica, foram abordados temas relacionados com a segurança da informação, *frameworks* (IDC, COBIT, ITIL), norma ISO 27001 e proteção de dados. Durante a análise da situação atual com recurso a análise de documentos atuais, políticas, procedimentos, instruções de trabalho e também recorrendo a entrevistas de colaboradores, identificaram-se várias oportunidades de melhoria, destacando-se a: falta gestão de mecanismos, auditorias internas, inexistência de cultura de participação ativa no tema, gestão de identidades e acessos, práticas de gestão de problemas, inexistência de avaliações á segurança de informação de parceiros externos, ausência de abordagens á gestão de risco, entre outras falhas.

Tendo em conta a avaliação da situação atual, procedeu-se ao desenvolvimento de um plano de iniciativas. Estas iniciativas foram construídas de forma a cumprir os requisitos da norma internacional ISO 27001 e do RGPD, tendo como referência o modelo de governança COBIT 5 e capaz de providenciar um serviço de alta qualidade segundo a estrutura ITIL. A melhoria do nível de segurança das tecnologias de informação permitirá uma melhoria na eficiência operacional e financeira, o cumprimento legal e regulamentar e aumento reputacional e comercial, para além de melhorar a capacidade de resposta a ameaças, quer internas e externas, aos sistemas de informação.

Após o cumprimento do plano estratégico, de ambos os *roadmap*, espera-se um aumento do nível de maturidade de segurança de 62%, um aumento da cobertura da norma internacional cerca de 144% e um aumento da cobertura do RGPD de 138%.

PALAVRAS-CHAVE

COBIT 5, ISO 27001, RGPD, Segurança da Informação

ABSTRACT

This dissertation entitled "Roadmap for Information Security applied to a Logistics Enterprise" was written in the context of the achievement of a master´s degree in Industrial Management and Engineering, to describe the research project developed in Rangel Logistics Solutions. This project arose from the fact that the company not only desired to acquire an ISO 27001:2013 international certification, but also to improve the maturity level of IT security – which is the main objective of this dissertation – and, consequently, have total compliance to the GDPR.

The investigation methodology followed was "Action-Research". Starting with the literature review, topics related to information security, several frameworks (IDC, COBIT, ITIL), ISO 27001 standard and data protection were explored. While assessing the current state by analysing latest documents, policies, procedures, work instructions and also by interviewing employees, several opportunities of improvement were identified such as lack of mechanism management, lack of internal audits, non-existence of active participation culture in formation security, lack of identity and access processes management, lack of problem management, non-existent assessment to the information security of external partners, and absence of a risk management approach, among many others.

According to the current state assessment, a plan of initiatives was developed. These initiatives were created in order to comply with the ISO 27001 standard and GDPR requirements, having as a reference the COBIT 5 governance framework and capable of providing high quality services according to the ITIL framework. The improvement of the security maturity level of IT will enable a better operational and financial efficiency, legal compliance, and commercial and reputational growth, besides improving the threat response, both internal and external, to information systems.

After the implementation of the strategic plan, a growth of the security maturity level is expected worth 62%, a growth of the international standard coverage worth around 144% and a growth of the GDPR coverage worth around 138%.

KEYWORDS

COBIT 5, GDPR, Information Security, ISO 27001

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

ISO/IEC	*International Organization for Standardization/International Electrotechnical Commission*
IEC	*International ElectroTechnical Commission*
TI	Tecnologias de Informação
SGSI	Sistema de Gestão de Segurança da Informação
PDCA	*Plan – Do – Check - Act*
RGPD	Regulamento Geral de Proteção de Dados
EU	União Europeia
COBIT	*Control Objectives for Information and related Technology*
ISACA	*Information Systems Audit and Control Association*
ITIL	*Information Tecnology Infrastructuture Library*
CCTA	*Central Computer and Telecomunications Agency*
OGC	*Office of Government Commerce*
LoB	*Line of Business*
B2B	*Business-to-business*
VoC	*Voice of Costumer*
B2C	*Business-to-consumer*
IDC	*International Data Corporation*
TCO	*Total Cost of Ownership*
ITSM	*Information Technology Service Management*
DPIA	*Data Privacy Impact Assessment*

1. INTRODUÇÃO

No primeiro capítulo da presente dissertação será realizado o enquadramento do tema "Roadmap para a Segurança de Informação numa empresa de Logística", efetuada no intuito de conclusão do plano de estudos do 5º ano do Mestrado Integrado em Engenharia e Gestão Industrial. Quer os objetivos propostos, quer a metodologia de investigação utilizada para este projeto e estrutura do documento, são apresentados de seguida.

1.1 Enquadramento

Os níveis de desempenho exigidos às empresas estão em constante crescimento, obrigando-as continuadamente encontrar formas de melhoria, de forma a atingir a perfeição.

Esta filosofia, juntamente com o aumento das ameaças à segurança da informação, que chegam de várias formas, não só ameaças externas através de ciberataques, mas também ataques comuns internos, como violações acidentais e erro humano, obriga as organizações a presenciarem-se de um plano capaz de suportar a continuidade da atividade de negócio, como também estar em conformidade com os parâmetros de clientes, parceiro e da Lei.

A Rangel Logistics Solutions, partilha essa visão, pelo que, também reconheceu que está bastante vulnerável, na medida que apresenta um nível de maturidade baixo no âmbito da segurança da informação, e, como tal, pretende melhorar esse nível.

1.2 Objetivos

Esta dissertação tem como objetivo principal, tal como o nome mostra, delinear um "*Roadmap*" (um mapa de estrada, um caminho, percurso, de modo a melhorar o nível de segurança da informação de uma empresa no setor da logística. De modo a cumprir este objetivo geral do projeto, foram traçados os seguidos objetivos suplementares:

- Identificação da visão geral da organização em relação ao cobrimento do plano de segurança da informação;
- Identificação e estabelecimento dos objetivos organizacionais em relação à empresa e mais especificamente, em relação às tecnologias de informação;

- Avaliação do estado das tecnologias de informação e consequente diagnóstico da situação atual, identificando falhas existentes;
- Projeção de um possível estado futuro de maturidade ao nível da segurança das tecnologias de informação
- Delineação de iniciativas adaptadas ao novo estado das tecnologias de informação;
- Análise do espaçamento entre o estado novo futuro e uma cobertura total da norma internacional ISO / IEC 27001:2013;
- Delineação de um novo plano de iniciativas para uma conformidade total da norma internacional e otimização da conformidade com o Regulamento Geral de Proteção de Dados;

Com o cumprimento do objetivo principal deste projeto, é pretendido obter os seguintes resultados:

- Melhoria do nível de maturidade de segurança dos sistemas de informação;
- Cobertura total dos requisitos e controlos da norma internacional ISO / IEC 27001:2013 e uma possível certificação futura;
- Conformidade com o Regulamento Geral de Proteção de Dados
- Aumentar a eficiência do trabalho na resposta a incidentes e reduzir custos associados;
- Obter processos normalizados

1.3 Metodologia de Investigação

O plano de Investigação em causa irá reger-se pela estratégia de investigação "*Action Research*", também denominado como "Investigação-Acão", visto que se trata de uma investigação ativa gerada por propósito inserida num contexto prático (direção de sistemas de informação da Rangel Logistics Solutions), e esta metodologia é caracterizado pela resolução de problemas operacionais bem como pela obtenção do conhecimento consequente das várias ações concretizadas ao longo do período de investigação. Além disso, segundo Saunders, Lewis e Thornhill (Mark Saunders, Philip Lewis, 2012), com esta estratégia é esperado um certo envolvimento do investigador com a organização e alguns dos seus colaboradores da organização, verificando-se uma participação ativa no tópico em estudo, criando-se um ambiente colaborativo entre todos para promoção de "mudança" na organização. Consequentemente, espera-se observar as implicações desta pesquisa em projetos futuros, isto é, os resultados alcançados devem ser passíveis de ser utilizados noutros contextos.

Assim, esta metodologia é composta por cinco fases sequenciais de um ciclo iterativo (O'Brien, 1998) fases estas que servirão de base para a elaboração da dissertação:

- Diagnóstico: Esta fase consiste numa análise crítica e avaliação da maturidade de segurança das tecnologias de informação do estado inicial das tecnologias de informação. Como auxílio ao diagnóstico, foram utilizadas ferramentas de avaliação;
- Planeamento das ações: Após identificadas as oportunidades de melhoria, foi elaborado um plano de ações, com vista a alcançar o estado desejado de maturidade para as tecnologias de informação;
- Implementação das ações: Implementação prática das ações delineadas nas iniciativas propostas;
- Avaliação dos resultados: Esta fase compreendeu a análise e avaliação dos resultados esperados com as ações descritas anteriormente, realizando-se uma comparação entre o estado futuro desejado e estado inicial de maturidade de segurança das tecnologias de informação.
- Especificação da aprendizagem: Por fim, identifica-se as descobertas e conclusões gerais da investigação e documentação de todo o processo realizado, de modo a permitir dar continuidade a este trabalho futuro.

Inicialmente, antes de dar início ao projeto de dissertação, deu-se início à revisão da literatura, permitindo ao investigador estar contextualizado e aprofundar os seus conhecimentos das temáticas relacionadas com a área de intervenção. Além disso, foi fundamental documentar toda a aprendizagem resultante do projeto realizado (elaboração da dissertação), processo este que se realizou em simultâneo com as tarefas mencionadas anteriormente.

1.4 Estrutura da Dissertação

O documento aqui presente está organizado em vários capítulos, sendo no total 9: Introdução, Revisão Bibliográfica, Apresentação da Empresa, Descrição e Análise do Processo, Oportunidades de Melhoria e Análise do Estado Futuro, Iniciativas, *Roadmaps* e requisitos de Controlo, Ações Executadas e Resultados e Conclusões e Propostas de Trabalho Futuro.

O primeiro capítulo, o atual – Introdução – é constituído pelo enquadramento do tema da dissertação, objetivos, metodologia de investigação e a estrutura do documento (atual subcapítulo).

No capítulo 2, é feita uma revisão bibliográfica que contempla os conceitos teóricos e fundamentais que servem de base para o projeto.

O terceiro capítulo descreve a organização hospedeira deste projeto: a *Rangel Logistics Solutions*, para além da visão da empresa sobre a temática da dissertação.

No capítulo 4, é feita uma avaliação da situação atual das tecnologias de informação ao nível da segurança da informação.

O quinto capítulo, estão apresentadas as oportunidades de melhoria na organização e estabelecimento dos novos níveis para um novo estado de maturidade das tecnologias de informação.

No capítulo 6 procede-se à apresentação de propostas de iniciativas para alcançar o nível de maturidade estado futuro.

No sétimo capítulo, é apresentado a proposta dos respetivos *roadmaps* de modo a cumprir as iniciativas propostas no capítulo anterior.

O oitavo capítulo apresenta as ações realizadas de modo a cumprir o plano das iniciativas propostas no capítulo 6.

Por fim, no último capítulo (capítulo 9) são expostas a conclusões finais deste projeto de investigação, incluindo reflexões acerca do cumprimento dos objetivos, dificuldades/limitações experienciadas e também incluindo sugestões para alguns pontos de trabalho que merecem alvo de estudo futuramente.

2. Revisão Bibliográfica

Neste capítulo é constituído pela revisão bibliográfica, que por sua vez apresenta os conceitos fundamentais que servem como base para o desenvolvimento da presente dissertação. Primeiramente, é introduzido o conceito de segurança da informação, como foco principal, uma vez que também é o tema deste projeto, sendo apresentados os seus pilares e a separação entre segurança da informação e cibersegurança. De seguida, serão apresentados um enquadramento da ISO/IEC 27001, à família de normas a que pertence e o Regulamento Geral de Proteção de Dados. Por fim, finaliza-se a revisão bibliográfica, de forma serão apresentados alguns *frameworks* de referência, como o *IDC Maturyscape*, o *COBIT* e o *ITIL*.

2.1 Segurança da Informação

Nos últimos anos, o termo Segurança da Informação começou a aparecer com maior frequência no escopo das organizações, mesmo que, por vezes, o seu conceito e objetivo não sejam totalmente compreendidos. No entanto, a segurança da informação é um aspeto crítico e desempenha um papel de proteção de negócio. As organizações devem proteger a sua informação e ativos de forma a sustentar o valor da empresa e respetiva reputação comercial (AlGhamdi et al., 2020). Hoje, os riscos relacionados com a segurança da informação são um grande desafio para as empresa, uma vez que alguns desses riscos podem levar a graves consequências, incluindo vulnerabilidade corporativa, perda de credibilidade, e dano monetário (Cavusoglu et al., 2004). Basta apenas uma violação da segurança bem-sucedida pelo infrator, como um roubo de dados, erro humano, ataque informático ou apenas um vírus informático nos sistemas de informação de uma organização, podem resultar numa severa perda de financeira e dano reputacional. Consequentemente, entidades reguladoras, funcionários, clientes e fornecedores estão preocupados com a segurança e privacidade da informação das organizações (Hardy, 2006).

Frequentemente, a segurança da informação é vista como um sinónimo de cibersegurança e como tal associada a uma temática meramente tecnológica que pode ser reduzida à expressão de compra e implementação de plataformas tecnológicas e que não existe a necessidade de escalar o tema a toda a organização.

Com a introdução de temas como o Regulamento Geral de Proteção de Dados (RGPD) (também introduzido nesta dissertação num dos capítulos seguintes) traz consigo o benefício de despoletar momentos de reflexão nas empresas, e, assim, trazer de alguma forma a consciência que a segurança

de dados e da informação, são muito mais que apenas de controlos técnicos, mas também, e principalmente, comportamentos humanos.

Existem evidências que frequentemente, projetos organizacionais começam sem qualquer abordagem em relação à segurança da informação, mesmo quando alguns riscos podem comprometer a o projeto e imagem comercial da organização. O problema principal é que as pessoas continuam a pensar que os sistemas e informação estão seguros, apenas pela pelo facto, de terem feito algum investimento nesses mesmos sistemas, pelo que, isso constitui um grande erro. Assume-se que, por muito investimento que se faça para manter os sistemas de informação atualizados, parece que nunca é suficiente para evitar o roube dados, divulgação de informação, a exploração de sistemas e outros riscos que são intrínsecos à informação suportados por redes e sistemas de informação. É um ciclo vicioso sem término, pelo que é necessário ser resiliente (de Oliveira Albuquerque et al., 2016). Além disso, evidências empíricas demonstram que o número de incidentes relacionados com a segurança da informação está de facto, a aumentar, apesar das organizações terem realizado grande investimento em soluções baseadas em tecnologia. Uma segurança de informação de sucesso pode alcançada através de um investimento, quer em recursos técnicos, quer em recursos socio-organizacionais.

Assim, segurança da informação pode ser definida como um conjunto de medidas técnicas, humanas e organizacionais que visam assegurar **três propriedades** dos dados e informação detida por uma organização, comumente conhecida como confidencialidade, integridade e disponibilidade, ou também como a tríade CIA (*Confidentiality, Integrity and Availability*), nome original na língua inglesa. A tríade CID (em língua portuguesa) são os três pilares ou princípios da segurança da informação (Samonas & Coss, 2014; Zafar et al., 2016):

- **Confidencialidade:** o termo "confidencialidade" é derivado do termo em latim "*confidere*", que significa ter total confiança ou confiabilidade. Confidencialidade é o primeiro princípio da segurança da informação. Esta é a propriedade que concede a proteção da informação do acesso indevido de terceiros. Assim, apenas as entidades autorizadas pelo proprietário da informação podem aceder e trabalhar com essa mesma informação.
- **Integridade:** o termo "integridade" significa solidez, totalidade e é derivado do termo em latim "*tangere*", que significa "toque" ou "tocar". Esta propriedade é dirigida à consistência, exatidão e credibilidade dos dados ao longo de todo o seu ciclo de vida, garantindo assim, que a informação manuseada mantém todas as usa características

originais, assegurando, assim, que a informação e programas só são criados e modificados numa maneira especifica e autorizada;

- **Disponibilidade:** o termo "*availability*" ("disponibilidade" na língua oficial inglesa) é derivado do termo em latim "*valere*", que significa "valer". Na informação da segurança, o termo "disponibilidade" significa "acesso e uso oportuno e confiável da informação". Esta propriedade garante que a informação esteja sempre disponível para o uso legítimo, aquando de uma entidade autorizada necessita o seu acesso.

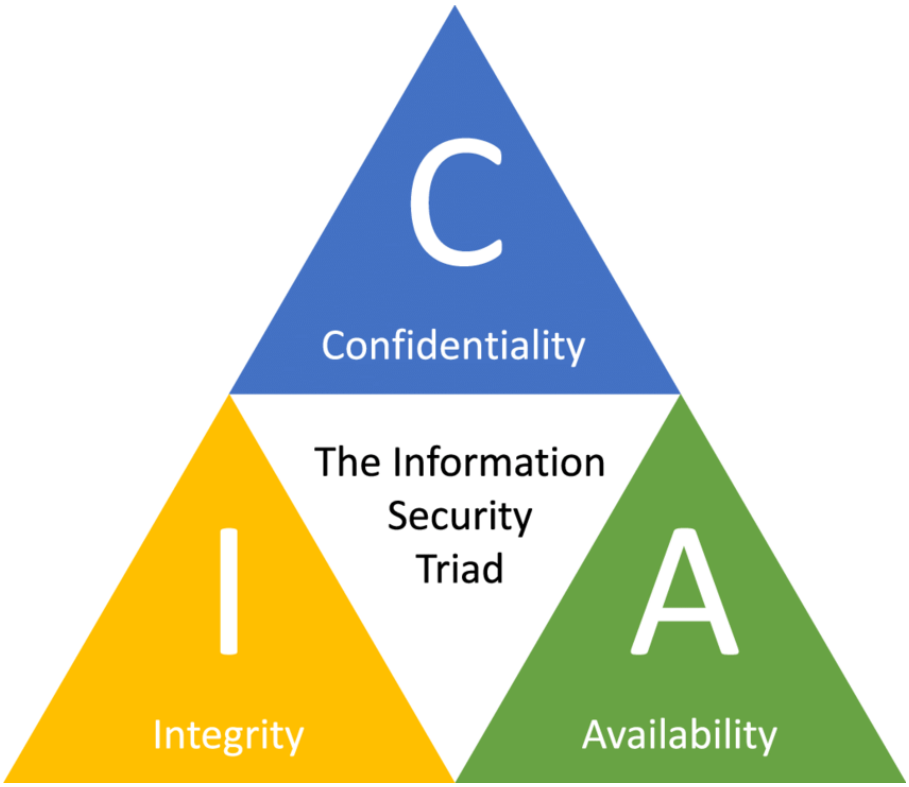


Figura 1 - The CIA triad (em português, a tríade CID)

Fonte: (Samonas & Coss, 2014)

Apesar de aplicável a qualquer setor de atividade, enquanto *input* de muitos serviços e produtos, a informação deve ser considerada um ativo estratégico pelos operadores logísticos. Ainda que o seu valor seja difícil de apurar, a utilização deste bem intangível é um dos desafios para estas empresas, no sentido de se adaptarem às macrotendências da logística, as quais assentam na transparência, rastreabilidade, segurança e otimização. Diretamente relacionada com a atividade logística, os dados e especialmente a informação são fundamentais para a execução eficiente das operações que se convertem em elevados níveis de serviço e como tal um elemento distintivo perante os concorrentes. Para tal, é necessário um correto e adequado modelo de governança e um rigoroso modelo de gestão dos sistemas que lidam com

a informação. Ineficiências ou problemas na qualidade e/ou fiabilidade dos dados e da informação traduzem-se em perda de competitividade de um operador logístico.

Em organizações com as suas operações fortemente suportadas em sistemas de informação e canais digitais na relação com os seus parceiros, a segurança dos sistemas de informação no sentido da salvaguarda do seu bom funcionamento deve ser expandida para algo mais abrangente como a Segurança da Informação. Ao longo deste estudo serão abordadas e discutidas temáticas de segurança das tecnologias de informação TI e cibersegurança, temas muito específicos de controlos técnicos para determinadas disciplinas das TI, porém como partes relevantes do âmbito maior que é a Segurança da Informação.

2.2 A Norma ISO/IEC 27001 e sua Origem

2.2.1 IS0, IEC e a família ISO/IEC 27000

Fundada em 1946, a ISO é uma organização com vestígios em 166 países. Foi criada por um grupo relativamente pequeno, maioria engenheiros de formação, sendo uma proeminente parte deles, britânicos e norte-americanos, dando-lhe o nome de *International Organization for Standardization* (Accerboni & Sartor, 2019).

A ISO desempenha um papel fundamental no auxílio do avanço tecnológico e industrial, bem como na normalização de padrões de produção e consumo, apesar de mesmo assim, ser uma instituição relativamente oculta. Com sede em Genebra, Suíça, é uma instituição não governamental, fazendo a ligação entre os setores privado e público, e além disso, é auto denominada como norma internacional para "negócios, governo e sociedade", por meio da sua perseguição de padrões voluntários,

A organização tem como objetivo a promoção da harmonização universal, de forma a eliminar barreiras que causam entravas no comércio mundial, exprimindo, assim, um consenso nos diferentes países com o propósito de facilitar esse mesmo comércio. Os membros ISO são as principais organizações de normalização em cada país e há apenas um membro por país. O representante em território nacional é o Instituto Português da Qualidade(Accerboni & Sartor, 2019).

Por outro lado, o *IEC - International ElectroTechnical Commission* foi fundado em St. Louis em 1904, sendo o precedente da ISO. A primeira reunião foi conduzida pela *British Institution of Electrical Engineers,* participando apenas 16 países, sendo três deles não europeus, Estados Unidos da América, Canadá e Japão. Em 1947, o IEC resolveu afiliar-se à ISO, começando de imediato, a cooperar como a divisão elétrica da própria ISO, mantendo-se, no entanto, como uma parte autónoma. A partir desse dia,

as duas organizações embarcaram numa cooperação que ainda se mantém até os dias de hoje (Eicher et al., 1997).

Por fim, emitida em 2009, a ISO / IEC 27000 refere-se à família de normas publicadas pela colaboração entre a *International Organization for Standardization* (ISO) e *International ElectroTechnical Commission* (IEC), de forma a fornecer um panorama da família de normas ISO 27000 e um conceito base genérico; como pode comprovar o seu título "*IT - Security techniques - Information security management systems - Overview and Vocabulary*". Além disso, fornece recomendações de práticas de gestão de segurança da informação, com objetivos de controlo, controlos específicos, requisitos, orientações para uma gestão de risco e controlo de segurança dentro do contexto de um Sistema de Gestão de Segurança da Informação (SGSI) (Disterer, 2013).

Tal como outras normas, esta família de normas assenta numa abordagem clássica, bem conhecida na gestão de qualidade criada por Deming, o ciclo "PDCA" (*Plan-Do-Check-Act*), como se pode observar na figura 2.

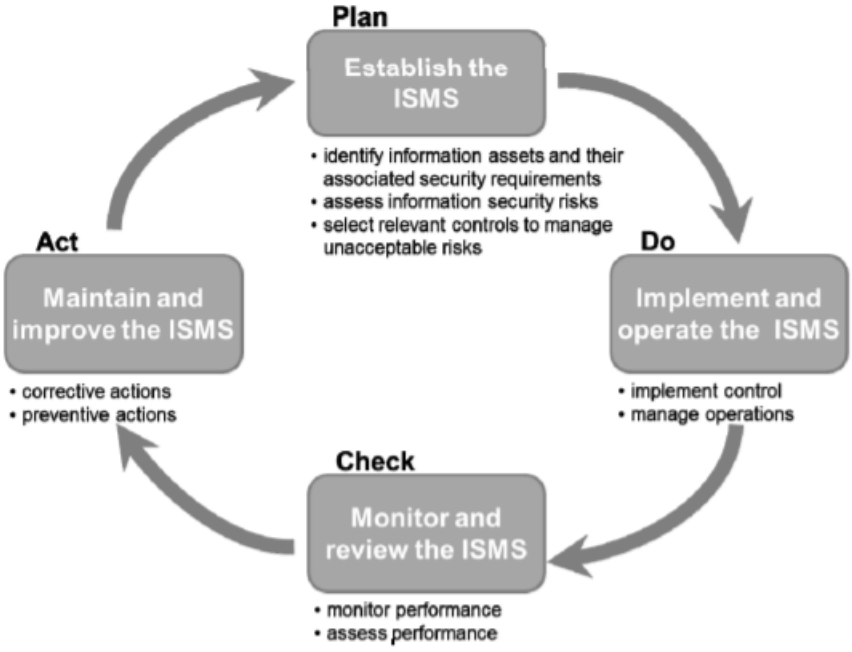


Figura 2 - Ciclo PDCA na ISO 27 000

Fonte: (Disterer, 2013)

O ciclo PDCA tem como objetivo incrementar a eficiência nas organizações, de modo a resolver problemas, tendo como base a promoção da melhoria contínua. O ciclo deve ser aplicado a todos os processos e SGSI como um todo.

Segundo *Deming*, de modo que a resolução de um problema decorra de forma eficaz, deve-se seguir os seguintes passos (Qusef et al., 2018):

- **Planear** (*Plan* na língua inglesa): Definir os requisitos para a proteção da informação, tal como os sistemas de informação asserem assegurados, identificar e avaliar os riscos, bem como estabelecer processos e medidas de redução dos mesmos. Ou seja, esta fase envolve a elaboração de estratégias de políticas e controlos de segurança necessários, sendo esta fase crucial, uma vez que é feito o mapeamento da visão inicial dos níveis de segurança da informação desejados pela organização.
- **Executar** (*Do* na língua inglesa): As ações definidas na fase inicial são implementadas. Esta fase abrange todas as implementações técnicas necessárias para obter um sistema de segurança da informação funcional, planeado na fase anterior.
- **Verificar** (*Check* na língua inglesa): Verificar o desempenho das ações implementadas através de uma monitorização ativa. Ou seja, com os resultados reportados, estabelecer termos de comparação com as metas delineadas anteriormente. Assim, esta fase envolve avaliações técnicas necessárias para assegurar uma funcionalidade de longo prazo ao sistema de segurança de informação, bem como os procedimentos de auditoria de segurança a serem seguidos para a garantia continua do nível de segurança do sistema dentro da empresa.
- **Agir** (*Act* na língua inglesa): Agir sobre o que foi verificado para melhorar o desempenho até que o problema inicial não se verifique. Esta fase envolve a preservação da qualidade do nível de garantida de segurança com base no *feedback recebido na fase "verificar"*, novas atualizações ou implementações que possam ser promovidas com base em novas adições ao sistema ou ameaças descobertas e resultados de avaliações de risco.

Esta família de normas representa uma coleção, não só recente, mas também bem-conhecida, que é retrabalhada e revista, de forma as normas estarem atualizadas e harmonizar o seu conteúdo e formato. Esta coleção tem como objetivo de possuir normas coesas na área da segurança da informação, além de compatibilidade com outros várias normas. Assim, é possível oferecer o apoio abrangente a organizações de todos os tamanhos, setores e tipos em assegurar a segurança da informação.
Por meio do uso da família de normas do SGSI, as organizações podem desenvolver e implementar uma estrutura para gerir a segurança dos seus ativos de informação. (Disterer, 2013)
Lista de normas da família ISO/IEC 27000:

- ISO/IEC 27000, *Information security management systems - Overview and vocabulary*

- ISO/IEC 27001, *Information security management systems – Requirements*
- ISO/IEC 27002, *Code of practice for information security management*
- ISO/IEC 27003, *Information security management system implementation guidance*
- ISO/IEC 27004, *Information security management - Measurement*
- ISO/IEC 27005, *Information security risk management*
- ISO/IEC 27006, *Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27007, *Guidelines for information security management systems auditing*
- ISO/IEC TR 27008, *Guidelines for auditors on information security controls*
- ISO/IEC 27010, *Information security management systems for inter-sector and inter-organizational communications*
- ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*
- ISO/IEC 27013, *Guidance on the integrated implementation of ISO/IEC 20000-1*
- *and ISO/IEC 27001*
- ISO 27014, *Proposal on an information security governance (ISG) framework*
- ISO/IEC TR 27015, *Information security management guidelines for financial services*
- ISO/IEC TR 27016, *Information security management - Organizational economics*
- ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*
- ISO/IEC 27034:2011, *Information technology - Security techniques - Application security*

Para além destas normas, existem mais que pertencem à família de normas 27 000, que estão presentes nos anexos deste documento.

2.2.2 NP ISO/IEC 27001:2013 e SGSI

A publicação da NP ISO / IEC 27001:2013 é a versão portuguesa idêntica à versão original ISO/IEC 27001, *Information security management systems – Requirements,* publicada (1° versão) em 2005. Esta versão foi criada como o objetivo de facilitar a sua aplicação em Portugal e nos países de língua oficial portuguesa.

A ISO/IEC 27001 é uma norma representa a estrutura de referência internacional para a gestão da segurança da informação tendo uma abordagem baseada no risco (Kurnianto et al., 2018), pelo que,

proporciona os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação, SGSI, dentro do contexto da organização (Beckers et al., 2013; En, 2015). Além de ser a norma mais conhecida da família, também é a única com possibilidade de certificação.

A ISO 27001:2013 sublinha 3 princípios ou "pilares" de segurança da informação eficaz: **pessoas**, **processos** e **tecnologia**. Esta abordagem com 3 vertentes ajuda as organizações a defenderem-se de ataques altamente organizados e ameaças internas comuns, como violações acidentais e erro humano. Assim, de acordo com a norma um SGSI apresentas as seguintes vantagens para as organizações:

- Permite a identificação e eliminação de ameaças e vulnerabilidades;
- Proporciona segurança e confiança a todos os *stakeholders* (clientes, parceiros e outras partes interessadas);
- Melhora a consciência de segurança;
- Aumenta a capacidade de prever, gerir e de sobrevivência a um desastre;
- Aprofunda o conhecimento sobre a própria organização e os eus respetivos processos, ativos e passivos;
- Fornece o conhecimento real do risco que a organização enfrenta;
- Contribui para a redução de custos e para melhoria dos processos e serviços;
- Garante o cumprimento da legislação em vigor;
- Reduz custos associados à "não segurança" (Lopes et al., 2019);

Origem e história

A norma internacional ISO 27001 sofreu várias e continuas alterações ao longo dos anos, tendo como origem duas normas previamente publicada e ambas britânicas, nomeadamente, a BS 7799 "*Information security management – Code of practice for information security management",* publicada em 1995 e a BS 7799-2: 1998 "*Information security management system – Specifications*", uma nova versão publicada em 1998. Ambas as normas foram criadas pelo *British Standard Institute*. Aliás, a sua origem primária é um documento publicado em 192 por um departamento do governo britânico que estabeleceu um código de práticas em relação à gestão de segurança da informação.

Em 2005, o comité da ISO/IEC publica uma primeira versão da norma internacional ISO/IEC 27001:2005, que não traz anda de novo e relevante em relação a uma versão anterior à norma britânica BS 7799-2:2002 (Accerboni & Sartor, 2019; Lopes et al., 2019)

Em 2013, há uma nova alteração ao documento, no entanto, essa alteração não é significativa.

Estrutura

Esta norma internacional é constituída por 10 capítulos, com a adição de um apêndice final, o "Anexo A". Os três primeiros capítulos referem-se ao "Objetivo e campo de aplicação", "Referências normativas" e "Termos e definições" evocando, assim, a norma ISO / IEC 27000, enquanto os capítulos seguintes, de 4 a 10, são dedicados aos seguintes requisitos estabelecidos pela norma:

- Contexto da organização
- Liderança
- Planeamento
- Apoio
- Operação
- Avaliação de desempenho
- Melhoria

A figura 3 mostra a numeração desses capítulos e consequente subcapítulos.

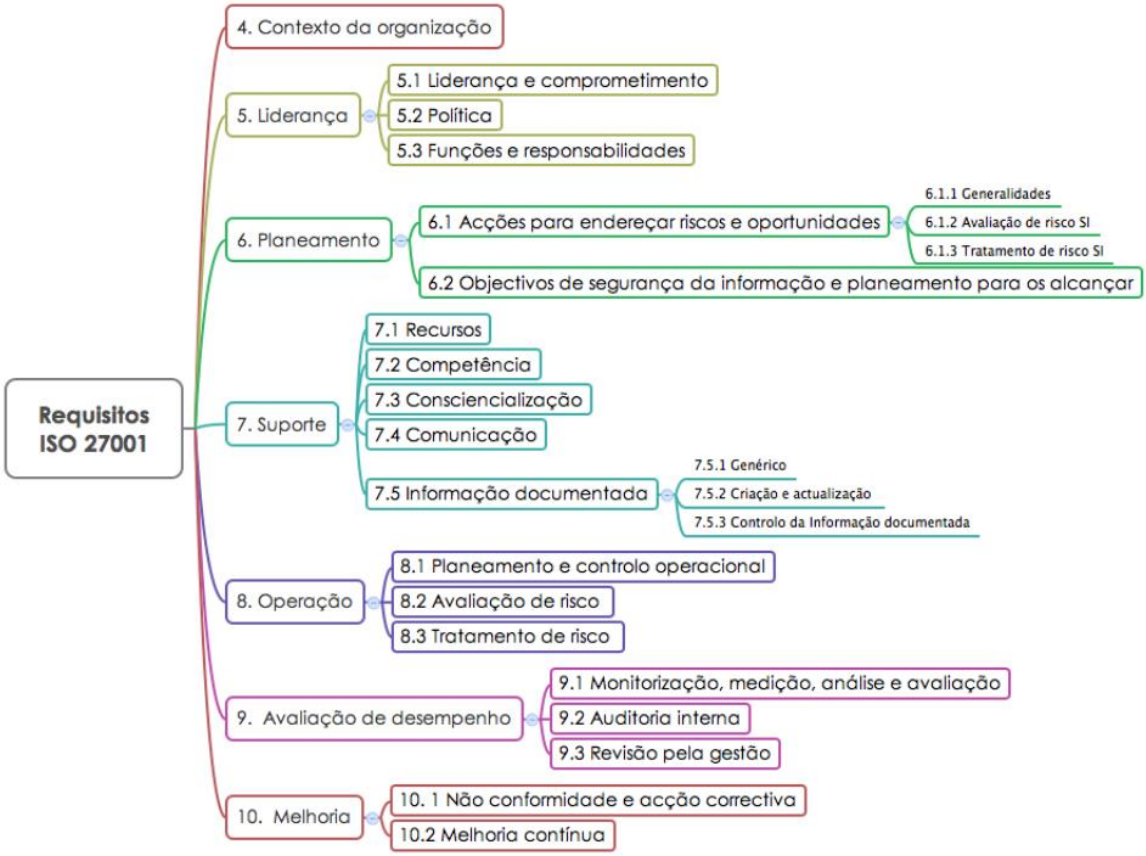


Figura 3 - Visualização geral dos capítulos (4 a 10) da NP ISO / IEC 27001:2013

Fonte: (En, 2015)

A segunda componente da norma, é denominada de "Anexo A" e é na realidade composta por um conjunto de controlos que as organizações devem adotar. Este apêndice tem 14 cláusulas de controlo de segurança, que ao todo contêm um total de 35 objetivos de controlos e 144 controlos. Ou seja, uma cláusula de controlo de segurança tem um ou mais objetivos de controlo, que define o que deve ser alcançado. Além disso, em cada objetivo de controlo é apresentado um ou mais controlos, que podem ser aplicados para alcançar esse mesmo objetivo de controlo.

Tabela 1 - Cláusulas e controlos da ISO 27001

Cláusulas	Descrição do Controlo de Referência (Anexo A)	Nº Objetvos	Nº Controlo
A.5	Políticas de Segurnaça 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	3	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 de Negócio	2	4
A.18	Conformidade	2	8

A tabela 1, enumera todas a cláusulas de controlo de segurança, objetivos de controlo que engloba e respetivos controlos do Anexo A na norma ISSO / IEC 27001:2013.

Por exemplo:

- A cláusula 10, conhecia pelo nome de "Criptografia", é constituída por 1 objetivo de controlo (A.10.1), e 2 controlos de segurança (A.10.1.1 e A.10.1.2).
- A cláusula 11, conhecia pelo nome de "Segurança Física e Ambiental" é constituída por 2 objetivo de controlo (A.11.1 e A.11.2), e 15 controlos de segurança.

2.3 Regulamento Geral de Proteção de Dados (RGPD)

O Regulamento Geral de Proteção de Dados é um regulamento introduzido pelo parlamento europeu, conselho europeu e comissão europeia, com entrada em vigor a 25 de maio de 2018, como objetivo de proteger os dados pessoais de todos os cidadãos europeus (Chaudhuri, 2016; Sirur et al., 2018). Até a essa data, os membros estados da união europeia seguiam as legislações nacionais de privacidade, de modo a seguir a diretiva 95/46/EC de 24 de outubro de 1995. Inevitavelmente, as diferentes interpretações originaram num conjunto de requisitos de conformidade de proteção semelhantes, mas não idênticos em toda o espaço europeu, o que permitiu às organizações tirarem partido dessa vantagem de territórios nebulosos de legislação e, consequentemente, procederam à exploração do uso destes dados (Diamantopoulou et al., 2020)

O RGPD permitiu melhorar o direito à privacidade dos indivíduos e possibilitou que os indivíduos da EU tivessem maior controlo sobre os seus direitos como o direito de acesso aos seus dados, retificação, apagamento, portabilidade, oposição e informação.

O regulamento obrigou as organizações que realizar algumas mudanças consideráveis na implementação da proteção da privacidade e como podem lidar com a informação dos seus clientes. Todos as

organizações, quer pertença à União europeia, quer não, que processam e tratam de dados pessoais de indivíduos residentes na União Europeia, devem cumprir as obrigações do regulamento. Consequentemente, as organizações não-UE e internacionais devem cumprir, não só com os seus regulamentos nacionais, mas também com o regulamento europeu (Hjerppe et al., 2019).

Contudo, a implementação do RGPD provoca grandes desafios nas organizações devido à falta de consciência e compreensão das mudanças necessárias e requisitos do próprio regulamento. Estes requisitos possuem várias implicações práticas de processos e práticas organizacionais, projeção de sistemas tecnológicos, como também treino dos colaboradores e distribuição de novas responsabilidades. Todo este processo global obriga as organizações a realizarem enormes esforços por parte dos colaboradores, como também um investimento financeiro elevado (Sirur et al., 2018).

Apesar do regulamento ter entrado legalmente em vigor só em maio de 2018, várias organizações foram multadas por não conformidade com o RGPD. O regulamento introduziu vários tipos de penalizações financeiras, superiores às existentes anteriormente. Os responsáveis pelo tratamento poderão ser condenados em multas cujo montante poderá ascender a **20 milhões de euros** ou a **4% do volume de negócios anual**, a nível mundial. Existe um sistema complexo de penalizações de acordo com a severidade da infração e responsabilidade do tratamento, existindo assim diferentes coimas para grandes empresas, pequenas e médias empresas e pessoas singulares. Além disso, o regulamento invoca responsabilidade civil, permitindo que qualquer titular de dados que tenha sofridos danos materiais ou imateriais em consequência de uma violação do RGPD tem direito a ser indemnizado pelos danos sofridos, e por outro lado, responsabilidade penal (Politou et al., 2018).

O RGPD tem uma estrutura complexa, sendo constituído por 99 artigos agrupados em 11 capítulos (Tikkinen-Piri et al., 2018). Estes últimos são:

1. Disposições gerais;
2. Princípios;
3. Direitos do titular dos dados;
4. Responsável pelo tratamento e subcontratante;
5. Transferências de dados pessoais para países terceiros ou organizações internacionais;
6. Autoridades de controlo independentes;
7. Cooperação e coerência;
8. Vias de recurso, responsabilidade e sanções;
9. Disposições relativas a situações específicas de tratamento;
10. Atos delegados e atos de execução;

11. Disposições finais

2.4 IDC MATURITYSCAPE - IT SECURITY 2.0

A estrutura de referência *MaturityScape - IT Security* foi criado pelo *International Data Corporation* (IDC), de modo a permitir uma avaliação das competências da arquitetura das redes de sistemas de informação, para além do nível de maturidade das organizações, no que diz respeito a cinco dimensões: **visão**, **gestão de risco**, **pessoas**, **processos** e **tecnologias de segurança.**

Este *framework* oferece aos gestores das organizações uma maneira estruturada, através uma explicação detalhada, para identificar o estado atual que uma organização se encontra, sendo possível catalogar desde um estágio simples e desordenado, o nível "*ad hoc*", até a um estágio avançado e sistematizado, o nível "*optimized*" (Gomes, 2018). Na totalidade, existem cinco níveis: *ad hoc*, *opportunistic*, *repeatable*, *managed* e *optimized,* como está representado na figura 4.

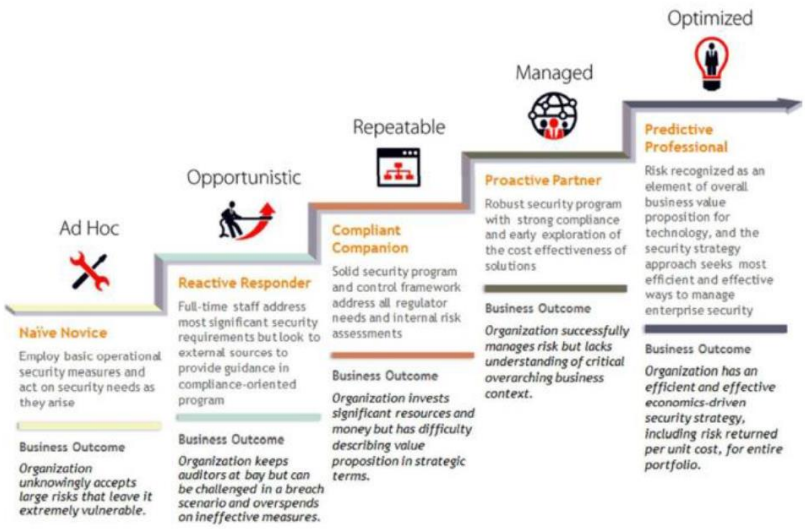


Figura 4 - Estágios da framework IDC MaturityScape – IT Security

Fonte: (Gomes, 2018)

2.4.1 Os níveis de maturidade de segurança dos sistemas de informação

Para cada estado apresentado é demonstrado o que uma determinada dimensão precisa de evoluir para promover a maturidade de segurança da informação das tecnologias de informação, permitindo, assim, encontrar a diferença entre o nível atual e nível que se deseja estar, de modo a manter o balanço competitivo e atingir superioridade industrial. Só assim será possível competir na nova era da transformação digital.

- ***Ad hoc***

- *Naïve novice*: Emprega medidas básicas de segurança operacional e atua nas necessidades de segurança à medida que surgem;

- ***Opportunistic***
  - *Reactive responder:* Uma equipa a tempo inteiro dedica a responder aos requisitos de segurança mais significativos, embora recorra a fontes externas para providenciar orientação.
- ***Repeatable***
  - *Compliant companion:* Um programa sólido de segurança e *framework* de controlo que responda a todos necessidade regulatórias e avaliações de risco internas;
- ***Managed***
  - *Proactive partner:* Um programa robusto de segurança que inclui forte conformidade e exploração antecipada das soluções custo-benefício;
- ***Optimized***
  - *Predictive professional*: O risco é reconhecido como um elemento da proposta geral do valor do negócio e a abordagem estratégica de segurança procura as formas mais eficientes e eficazes de gestão de segurança empresarial;

2.4.2 As dimensões da estrutura de referência

Como referido num dos subcapítulos anteriores, o *MaturityScape – It Security* é constituído por cinco dimensões, detalhas de seguida (Management, n.d.):

- **Visão:** Proporciona o contexto para as organizações de modo a incorporar as subdimensões para os objetivos de negócio, objetivos de segurança, supervisão regulatória e orçamentação numa numa abordagem coesa e estratégica para a gestão de risco tecnológica;
- **Gestão de Risco:** Retira os objetivos estratégicos de negócio da dimensão Visão e constrói os requisitos do programa de segurança numa maneira mais específica, de modo a direcionar as subdimensões para a abordagem do risco, metodologias e medições, relações externas e ambiente de controlo;

- **Pessoas:** Envolve os papéis de liderança executiva e cultural organizacional geral, desenvolvendo níveis de maturidade para executivos de segurança e segurança *outsourcing*;
- **Processos:** descreve as atividades que uma organização emprega, de forma a gerir o risco num ambiente operacional. Desenvolve-se sobre níveis de maturidade em 4 subdimensões: confiança, identidade, vulnerabilidade e gestão de ameaças;
- **Tecnologias de Segurança:** inclui os vários programas de segurança, de modo a proteger os recursos através de tecnologia em toda a arquitetura tecnológica para as subdimensões confiança, identidade, vulnerabilidade e gestão de ameaças:

2.5 COBIT e COBIT 5

2.5.1 COBIT

O COBIT (*Control Objectives for Information and related Technology*), é uma estrutura de referência reconhecida que se posiciona como uma ferramenta de governança e gestão de tecnologias da informação (ISACA, 2012; Nabil Almunawar et al., 2011; Othman et al., 2014; Von Solms, 2005). Esta *framework* certificada foi desenvolvida pela ISACA (*Information Systems Audit and Control Association)* e pelo Instituto de Governança TI (IT Governance Institute -ITGI) em 1996 (Nabil Almunawar et al., 2011; Othman et al., 2014) de modo a oferecer às empresas uma solução objetiva para alinhar as estratégias de negócio com os objetivos TI (Amorim et al., 2021).

Assim, esta *framework* é a melhor ferramenta no auxílio da implementação de estruturas organizacionais, princípios, governança estruturada e gestão de processos, alinhados com a visão da organização enquanto é fundamental na mitigação de riscos e adição de valor (Amorim et al., 2021).

Visto isto, pode-se considerar o COBIT como um conjunto de ferramentas de suporte que permite os gestores colmatarem o fosso entre os requisitos de controlo, questões técnicas, riscos de negócio e questões de segurança (Nabil Almunawar et al., 2011) tendo o foco na gestão e no controlo das tecnologias da informação (Kerr & Murthy, 2013).

2.5.2 Cobit 5

A atual e mais recente versão da *framework*, COBIT 5, consolida a versão anterior (COBIT 4.1), VAL IT e Risk IT, numa só *framework*, enquanto é atualizada para alinhar com as melhores práticas como o ITIL

e o *The Open Governance Architecture Framework* (TOGAF). Ambas a versões (4.1 e 5) podem ser usadas como guia para ajustarem o necessário para os processos das empresas.

O COBIT 5 é considerado adequado com base no seu espírito, que é definido por 5 princípios listados em baixo (Othman et al., 2014):

- **Princípio 1:** Satisfazer as necessidades das partes interessadas;
- **Princípio 2:** Cobrir todos os pontos *end-to-end* da organização;
- **Princípio 3:** Aplicar uma *framework* única e integrada;
- **Princípio 4:** Proporcionar uma abordagem holística;
- **Princípio 5:** Separar governança de gestão;

O ISACA desenvolveu esta nova versão para ajudar as empresas a implementar capacitadores de governança sólidos, oferecendo às organizações uma forma objetiva de alinhar as estratégias de negócio com os objetivos TI. Assim, a *framework* abrange 5 princípios, 7 capacitadores, 26 funções e 37 processos de gestão e governança e as suas boas práticas correspondentes, como as 7 fases sequencias (Amorim et al., 2021):

1. O que são impulsionadores?
2. Onde estamos agora?
3. Onde queremos estar?
4. O que é preciso ser feito?
5. Como é que chegamos lá?
6. Chegamos lá?
7. Como é que mantemos este impulso?

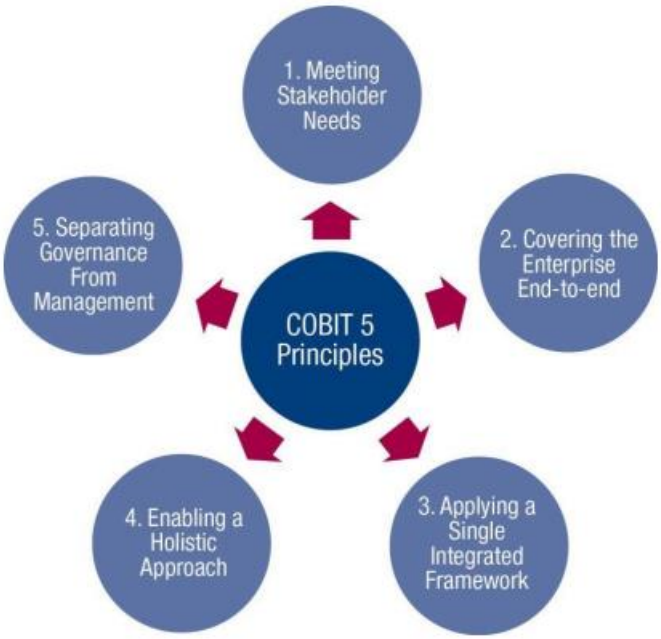


Figura 5 - Princípios COBIT 5

Fonte: (ISACA, 2012)

2.6 ITIL

2.6.1 Information Tecnology Infrastructuture Library (ITIL)

Nos últimos anos, as funções de tecnologias de informação foram obrigadas a tornaram-se mais orientadas ao serviço por uma confluência de circunstâncias (exigências externas, dependência nestas tecnologias, ect), pelo que, deste modo, pudessem se tornar melhores no alinhamento dos objetivos empresariais. Uma ITSM (*Information Technology Service Management*) é uma estratégia capaz de ajudar as organizações TI tornarem-se mais adaptáveis, flexíveis, rentáveis e orientada ao serviço, respondendo, assim, às exigências do mercado, sendo o ITIL a estrutura de referência de eleição (Pollard & Cater-Steel, 2009; W. G. Tan et al., 2009).

O conceito ITIL, *Information Tecnology Infrastructuture Library,* emergiu, uma primeira versão, nos anos 80' devido às sucessivas queixas do governo britânico relativamente à qualidade do nível de serviço TI fornecido, não corresponder às suas necessidades (Iden & Eikebrokk, 2013; McNaughton et al., 2010). Originalmente desenvolvida pelo governo britânico, mais concretamente, pela agência central de computador e telecomunicações (*Central Computer and Telecomunications Agency* em inglês ou CCTA) que agora é o atual gabinete de comércio governamental (*Office of Government Commerce* na língua

oficial inglesa ou OGC) (Pollard & Cater-Steel, 2009; W. G. Tan et al., 2009), o ITIL era uma coleção de livros, cerca de 40 volumes, cada um cobrindo uma prática e prática específica na gestão de serviços TI, para promover operações TI eficientes e rentáveis nos centros de computação controlados pelo governo (Pollard & Cater-Steel, 2009).

O ITIL é um conjunto de conceitos e das melhores práticas estruturadas e detalhadas para a gestão dos serviços das tecnologias da informação como um todo, na melhor qualidade possível, ordem e continuidade, de forma a garantir a máxima harmonização entre serviços TI e objetivos da empresa, conseguindo, assim, cumprir com as expectativas dos clientes ao mais alto nível possível (Ozdemir et al., 2014; Rezakhani et al., 2011; Wegmann et al., 2008).

O ITIL funciona como um *roadmap* para a melhoria de processos de forma a ajudar os profissionais de tecnologias de informação a criar a base para um serviço contínuo de excelência, ao mesmo tempo que cumpre os requisitos orçamentais e regulamentares (Pollard & Cater-Steel, 2009).

Por fim, o ITIL como qualquer ITSM providencia vários benefícios, entre os quais (Hochstein, 2005; W.-G. Tan et al., 2007):

- Melhoria na orientação Cliente/Serviço;
- Melhoria na qualidade dos serviços TI;
- Maior eficiência devido à estandardização;
- Otimização de processos;
- Automação de processos;
- Transparência e comparabilidade por documentação e monitorização de processos;
- Infraestruturas mais previsíveis;
- Melhoria na consultoria com os grupos TI da organização;
- Negociações mais tranquilas de acordo com o nível de serviço;
- Serviço *end-to-end* perfeito;

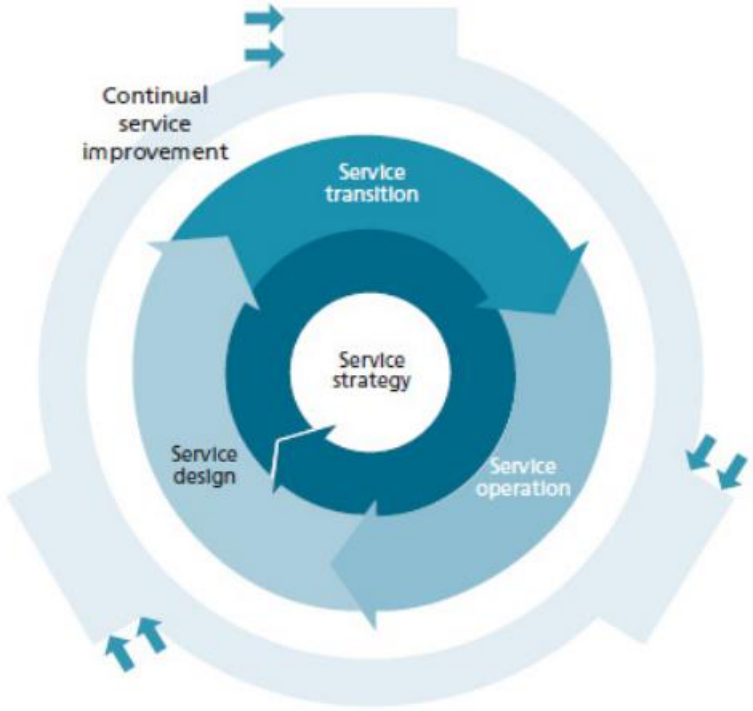


Figure 6 - Ciclo de vida do Serviço ITIL V3

Fonte: (Ferreira et al., 2016)

2.6.2 ITIL V3

O ITIL V3 foi criado em maio de 2007, tornando numa versão melhorada do ITIL V2, estendendo os processos do último e estruturá-los num modelo de ciclo de vida. Neste ciclo de vida, os serviços TI são projetados, criados, transacionados para um ambiente ativo, suportados operacionalmente, continuadamente melhorados e retirados no fim do seu ciclo de vida (W. G. Tan et al., 2009).

O ITIL V3 é constituído por 5 volumes (ou publicações) cada uma fornece orientação para cada fase especifica do ciclo de vida da gestão de serviços (Pollard & Cater-Steel, 2009; Sheikhpour & Modiri, 2012):

- **Estratégia**: Fornece orientação de como projetar, desenvolver e implementar gestão de serviços de uma perspetiva de capacidade organizacional e ativo estratégico. Útil no desenvolvimento de políticas, diretrizes e processos ao longo do ciclo de vida do serviço ITIL. Também é aplicável no contexto de outras fases do ciclo de vida. O Serviço Estratégico cobre as seguintes partes dos sistemas TI: desenvolvimento de mercados, interno e externo, ativos, catálogos e implementação da estratégia no ciclo de vida do serviço;

- **Desenho:** É a orientação para a criação e desenvolvimento de serviços e processos de gestão de serviços. Cobre os princípios e métodos de projeção de modo a converter objetivos estratégicos em portfólios de serviços e ativos de serviço. Inclui mudanças e melhorias necessárias para aumentar e manter valor para os clientes durante o ciclo de vida dos serviços, continuidade dos serviços, obtenção de níveis de serviço e conformidade com normas e regulamentos.
- **Transição:** É a orientação para o desenvolvimento e melhoria das capacidades para a transição de novos e mudança de serviços para operações. Orienta como os requisitos do Serviço Estratégico codificados no Serviço de Desenho são realizados eficazmente no Serviço de Operação enquanto se controla os riscos de fracasso e rutura;
- **Operação:** Incorpora práticas na gestão do Serviço de Operação. Inclui orientação na obtenção de eficácia e eficiência na entrega e suporte de serviços, de forma, a assegurar o valor para o cliente e fornecedor de serviço. Os objetivos estratégicos são finalmente realizados, tornando-se, assim, numa capacidade crítica;
- **Melhoria contínua:** Inclui orientação instrumental na criação e manutenção de valor para os clientes por um melhor desenho, introdução e operação de serviços. Combina princípios, práticas e métodos de gestão da qualidade e gestão da mudança e melhoria da capacidade. Organizações aprendem a realizar melhorias incrementais e em larga escala no serviço de qualidade, eficiência operacional e continuidade de negócio.

No ITIL V3, podemos encontrar mais informação em relação à orientação sobre a gestão da segurança, pois nesta versão, foi incluída no volume de Serviço de Desenho este processo, tendo o objetivo de alinhar a segurança das tecnologias de segurança com a segurança empresarial, além de assegurar que a segurança da informação é gerida eficazmente em todos os serviços e atividades de gestão de serviços (Taylor & East, 2013). Por isso, esta versão fornece um tratamento mais adequado à segurança que a Versão 2, identificando detalhes da estrutura e implementação dos processos de gestão da segurança da informação juntamente com as boas práticas para a implementação de um SGSI incluído numa norma ISO da família de série 27000 (Larrocha et al., 2010).

No total, as cinco fases do ciclo de vida são constituídas por 26 processos e 4 funções.

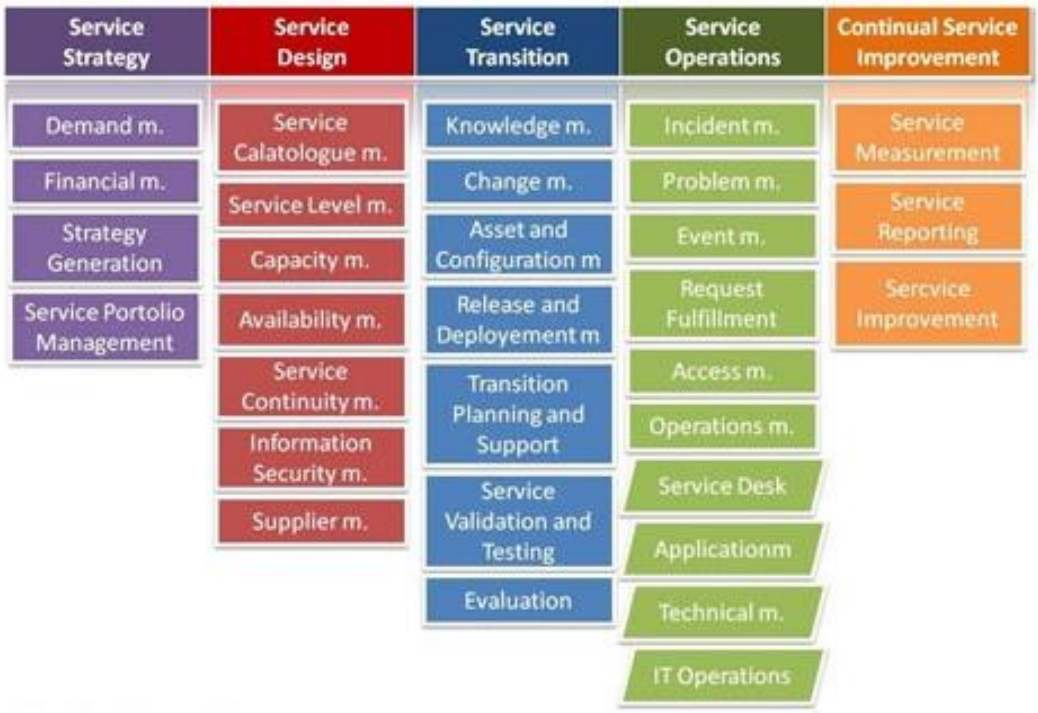


Figure 7 - Processos e Funções ITIL

Fonte: (Mahy et al., 2017)

3. Apresentação da Empresa

Neste capítulo, é realizado uma apresentação da empresa, onde este estágio curricular, e consequente projeto de investigação se desenvolveu. Inicialmente, começar-se-á por providenciar uma breve apresentação do Grupo Rangel, seguindo-se da sua história, a sua estrutura organizacional e clientes corporativos. Por fim, será feito um enquadramento do alvo de estudo da presente investigação com a visão da empresa.

3.1 O grupo Rangel

Fundada em 1980, a Rangel Logistics Solutions rapidamente marcou posição no mercado, sendo hoje reconhecida como um parceiro logístico global com capacidade de integração de uma vasta gama de serviços de transporte e logística, oferecendo ao mercado uma solução *One Stop Shop*.

Com cobertura mundial e apoiado por uma rede de parceiros globais, a Rangel movimenta mercadoria entre mais de 220 países e territórios por terra, mar e ar. Para além de Portugal, estão diretamente presentes em Angola, Moçambique, Cabo Verde, Brasil, África do Sul e México.

A Rangel Logistics Solutions é o parceiro olímpico do Comité Olímpico de Portugal como operador logístico oficial, assegurando toda a operação logística para os Jogos Olímpicos de Tóquio 2020, realizado em 2021.

Figura 8 - Grupo Rangel

3.2 História

Constituída em 1980, a Rangel rapidamente marcou posição como um dos mais ativos e inovadores grupos do setor. Ao longo dos seus 41 anos de história, o grupo diversificou a sua atividade para as mais variadas disciplinas da cadeia logística.

Figura 6 - De 1980 a 2009

Abrindo uma filial em Angola, a Rangel debutou-se na internalização 2017, seguindo-se Moçambique em 2011, Brasil em 2013, e Cabo Verde em 2015. Com "o objetivo de criar um triângulo logístico entre América, África e Europa", a Rangel Logistics Solutions instala-se no México em 2020, com o escritório central na Cidade do México com um Investimento inicial de 750 mil euros, esperando, no entanto, mais investimos futuros (previsão de abrir mais três escritórios, nos próximos dois anos) neste país.

Figura 7 - De 2011 a 2020

O ano de 2019 originou mais um movimento de crescimento relevante, com a parceria estratégica conjunta com os *Correos Expresso*, com vista a criar uma rede ibérica de transporte expresso com possibilidade de movimentar carga em 24h para qualquer ponto da Península Ibérica. Os *Correos* são líderes de mercado em Espanha, faturando, quase, 2 mil milhões de euros, com 51 mil colaboradores e movimentando, por dia, 11 milhões de despachos.

O grupo Rangel fechou o ano de 2020 com uma faturação na ordem dos 203 milhões de euros, mais cerca de 5% do que no ano anterior, e um efetivo a rondar os 2.100 trabalhadores.

3.3 Missão

A capacidade de oferta de uma solução logística integrada e global é o principal ativo da organização. Várias décadas de experiência, sistemas inovadores e uma equipa de profissionais apaixonados permitem à Rangel criar valor, inovação e contribuir para o progresso dos seus clientes.

As especificidades de cada cliente estão no centro da sua cultura de negócio. Desenhamos serviços únicos e adaptados às indústrias, construindo relações de longo prazo com os clientes.

Figura 8 - Valores da Rangel

3.4 Estrutura Organizacional

Rangel gere um portefólio diversificado de negócios na área dos transportes e logística, tendo uma presença em todo o globo. A organização é constituída por ramos de atividade (*Line of Business* – LoB): *Customs Broker*, *Road Freight*, *Air & Sea Freight*, *Internetional Express*, *Express & Parcels*, *Contract Logistics*, *Custom Critical* e *Feirexpo*), apresentando equipas com a maior competência e dedicação, para além de especializada, que em conjunto oferecem de forma integrada, soluções logísticas globais.

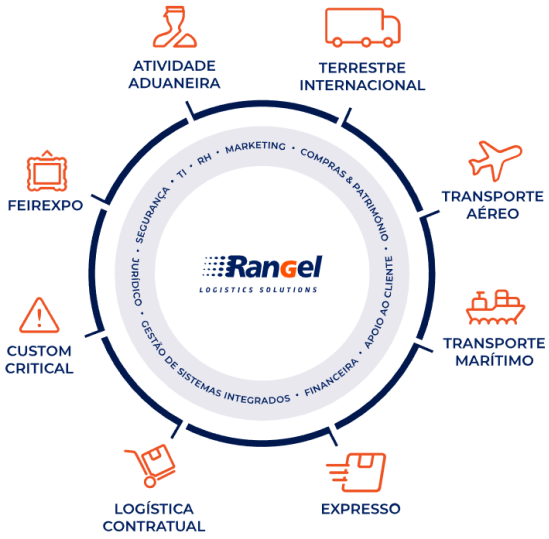


Figura 9 – Atividades de negócio do Grupo Rangel

Depois de proporcionar um nível de especialização elevado em cada nível da cadeia logística, permitindo assim alcançar excelentes níveis de serviço, A Rangel possui uma visão verticalizada por setor e/ou indústria que atravessa de forma transversal as várias áreas de negócio (*LoB*), de modo a assegurar os seus clientes e parceiros numa visão *end-to-end* de todo o seu processo logístico. Dessa forma a Rangel possui produtos especializados para os seguintes mercados verticais:

Figura 10 – Setores/indústrias de atividade

Relativamente à disposição geográfica direta, é evidente a aposta do Grupo Rangel nos PALOP, países africanos de língua oficial portuguesa, pelas óbvias razões da forte relação comercial entre Portugal e esses países, de modo a estimular o crescimento económico destes países, para além da presença no Brasil e México.

Figura 11 - Presença da Rangel no Mundo

Relativamente à sua distribuição geográfica em território Nacional, A Rangel apresenta uma forte presença no Norte através da sede de Folgosa, na Maia, para além do enorme parque logística no Montijo.

Figura 12 - Disposição geográfica da Rangel em Portugal

O diagrama abaixo ilustra o Grupo em números, com base em dados de 2020:

Figura 13 - Números Relativos ao ano de 2020

3.5 Clientes

Os clientes com as quais a Rangel colabora pertencem aos mais diversos setores de atividade, com um forte crescimento no setor farmacêutico, destacando-se os que se encontram na figura abaixo.

Figura 14 - Clientes constantes da Rangel

3.6 Segurança da Informação no grupo RANGEL

Atualmente, os riscos associados com a Segurança da Informação são um enorme desafio para as organizações, uma vez que esses riscos podem originar consequências desastrosas, incluindo responsabilidade corporativa, perda de credibilidade e danos financeiros. Consequentemente, assegurar a segurança da informação tornou-se um dos objetivos prioritários de gestão nas empresas, tanto nas

incumbentes como nas nativas digitais ainda que em graus de preocupação distintos mediante a dependência/adoção do digital pela organização.

Hoje em dia, as organizações confiam afincadamente nos sistemas de informação, então, aspetos como a resiliência dos sistemas de informação, as ciberameaças e mais recentemente pelas questões regulatórias impostas pelo RGPD, trouxeram para as agendas das empresas o tema, sendo comum atualmente, com especial enfoque em determinados setor de atividade, que uma estratégia para a Segurança da Informação seja um *order winner* (requisito valorizado para a contratação, capaz de ser decisivo na contratação para um serviço de logístico) ou mesmo um *order qualifier* (requisito para ser considerado para a prestação do serviço por um cliente).

Depois de bom processo VoC (*Voice of Costumer*) e leitura de mercado, o Grupo Rangel não é exceção e algumas características organizacionais determinam o elevado grau de importância que a Rangel deve dar à questão. Por conseguinte, foi delineado quatro objetivos organizacionais: legal, *business continuity*, melhoria da eficiência operacional e financeira, e comercial e reputacional. Estes objetivos encontram-se representados na seguinte imagem

Figura 15 - Objetivos Organizacionais

- **Legal:** a União Europeia colocou em vigor o RGPD, que introduz uma base ou conjunto de regras para as empresas que manuseiam dados, cujo proprietários são cidadãos europeus, motivando assim a Rangel a adotar uma estratégia para a segurança. Este conjunto de regras incide sobre o tratamento de dados pessoais de particulares e além disso, nenhuma área de negócio da Rangel, seu *core business*, é especificamente o tratamento desse tipo de dados. Mesmo se posicionando, maioritariamente, como um *player B2B*, o efeito crescente do e-commerce e do B2C, também impulsionado pela pandemia virológica de 2019, teve como consequência, o

crescimento dos dados pessoais de particulares que são sujeitos a tratamento nas atividades quotidianas de prestação de serviços de logística.

Adicionalmente, o Grupo Rangel é uma grande organização, aproximadamente, com 2300 colaboradores, internos e externos, que endereça temas de conteúdo sensível como a medicina no trabalho. Uma estratégia de segurança da informação planeada e implementada em toda em a organização é uma forma sustentada e robusta de alcançar a conformidade com o RGPD.

- **Business Continuity:** devido à elevada dependência dos sistemas de informação, o tema de continuidade de negócio e resiliência dos mesmos sistemas é um tema de elevada significância para a Rangel. Isto deve-se ao facto, de toda a atividade das várias *LoB* estrem completamente assentes em sistemas de informação. Quase todas as operações tecnológicas com recursos próprios, nomeadamente, infraestruturas *core* de *datacentres*, *networking* e comunicações, microinformática e desenvolvimento aplicacional, é efetuado, em grande parte, internamente. Num passado mais recente, adoção de medidas mais técnicas, como soluções na *cloud*, nomeadamente, *Saas*, tem tido uma expressão relevante sendo necessário assegurar de igual forma a gestão de contratos e monitorização de níveis de serviço. O *business continuity* é um dos objetivos organizacionais da Rangel devido a 3 motivos:
    - Elevada dependência nos sistemas de informação nas operações, para além do facto de operar $24 \times 7 \times 365$;
    - Grande dispersão geográfica, o que leva a várias diferenças de fuso horário;
    - A logística e distribuição de produtos farmacêuticos é um setor específico, que rege-se por regras e boas práticas muitos específicas, impostas por lei (diretriz 2013/C/68/01), o que obriga a um exigente controlo de alterações e disponibilidade;
- **Eficiência operacional e financeira:** a normalização e formalização de procedimentos operacionais internos presenteados pelas boas práticas de *frameworks* reconhecidas, transforma uma estratégia para a segurança da informação em eficiência operacional e, consequentemente, origina ganhos monetários. Estes benefícios podem ser traduzidos e quantificados através de ganhos financeiros e/ou ganhos operacionais, pela redução ou eliminação de retrabalho e esforço na resolução de problemas.
- **Comercial e Reputacional:** tal como na atividade de manutenção dos clientes e parceiros logísticos atuais, como na atividade de captação de novos contratos, é significativo o aumento da importância pelo tema da segurança da informação, para além de em alguns setores de negócio, um aumento da preocupação pela adoção de boas praticas reconhecidas, como por

exemplo, a própria ISO 27001:2013, pelo que, uma certificação da mesma, funcionar como order qualifier ou, até mesmo, order winner.

Com intuito de avaliar, o impacto do ganho/ perda comercial e reputacional, foi realizado um *assessment,* através da avaliação de uma pequena amostra de um conjunto de 10 clientes (n=10 clientes), de modo a aferir que sistemas de gestão eram valorizados e/ou requeridos, obtendo os seguintes resultados:

Tabela 1 - Requisitos dos clientes Rangel e respetivos volumes de negócio

Clientes	Setor de Atividade	Volume de Negócio em 2019	SI	CN	LoB
F*****	Pharma & Healthcare	689 880,00 €	x	x	Contractual Logistics
F*****	Pharma & Healthcare	299 364,00 €	x	x	Contractual Logistics
T*****	Pharma & Healthcare	303 900,00 €	x	x	Contractual Logistics
T*****	Pharma & Healthcare	945 439,00 €		x	Contractual Logistics
T****	Pharma & Healthcare	1 008 345,00 €		x	Contractual Logistics
L*****	Pharma & Healthcare	1 117 314,00 €		x	Contractual Logistics
E*****	Pharma & Healthcare	502 027,00 €		x	Contractual Logistics
G*****	Pharma & Healthcare	107 960,00 €	x	x	Contractual Logistics
G*****	Transport and Logistics	6 434 054,00 €	x	x	Air & Sea Freight
B*****	Transport and Logistics	203 244,00 €	x	x	Air & Sea Freight
	Total	11 611 527,00 €			

Legenda: SI – Segurança da Informação / CN – Continuidade do negócio

Nota: Para efeitos de confidencialidade, o nome dos clientes foi anonimizado.

Como se pode observar na **Error! Reference source not found.**, por meio da análise destes resultados, pode-se concluir que os clientes do setor farmacêutico criam uma enorme pressão toque toca à segurança da informação e à continuidade de negócio, que pode ser assegurada, no que diz respeito aos sistemas de informação, através da adoção de uma estratégia de segurança. Além disso, a receita anual desta amostra representa um valor superior a 11,6 M€, sustentado, desta forma, a relevância que a segurança da informação possui para a Rangel.

3.6.1 Alinhamento dos objetivos organizacionais com os objetivos TI segundo o COBIT 5

A estrutura de referência reconhecida de governança de TI, *COBIT 5*, faz o alinhamento crucial entre os objetivos empresariais com as soluções e serviços TI em relação ao tema de segurança da informação, assim como identificar métricas para avaliar a sua aplicação.

De modo a seguir os passos do mecanismo de *Goals Cascade* do *COBIT 5*, primeiramente foram mapeados os objetivos organizacionais da Rangel para a segurança de informação com os objetivos

empresarias (*Entreprise Goals* na língua oficial inglesa) da estrutura. De seguida, no passo seguinte, os objetivos empresariais são mapeados com os objetivos relacionados com as TI (*IT Related goals* na língua oficial inglesa).

No *Goals Cascade*, os objetivos empresariais só podem ser alcançados se os objetivos relacionados com TI forem encontrados, sendo que cada um dos 17 objetivos empresariais são mapeados com um número determinado de objetivos relacionados com as TI.

Por fim, no último passo, é necessário mapear os objetivos relacionados com as TI com os objetivos promotores (*enablers goals* na língua oficial inglesa). De modo a atingir os IT related goals, um número de *enablers* devem ser aplicados com sucesso. Um destes *enablers* é **Processos**. Tal como nos passos anteriores do *goals cascade*, cada objetivo relacionado com as TI é mapeado com um ou mais processos.

A *framework* COBIT 5 tem **17 objetivos genéricos** que são facilmente transformados em objetivos empresariais, **17 objetivos relacionados com as TI** e um total de **37 processos**.

Todo este processo é representado abaixo, estando os primeiros passos representados na *Figura 16*.

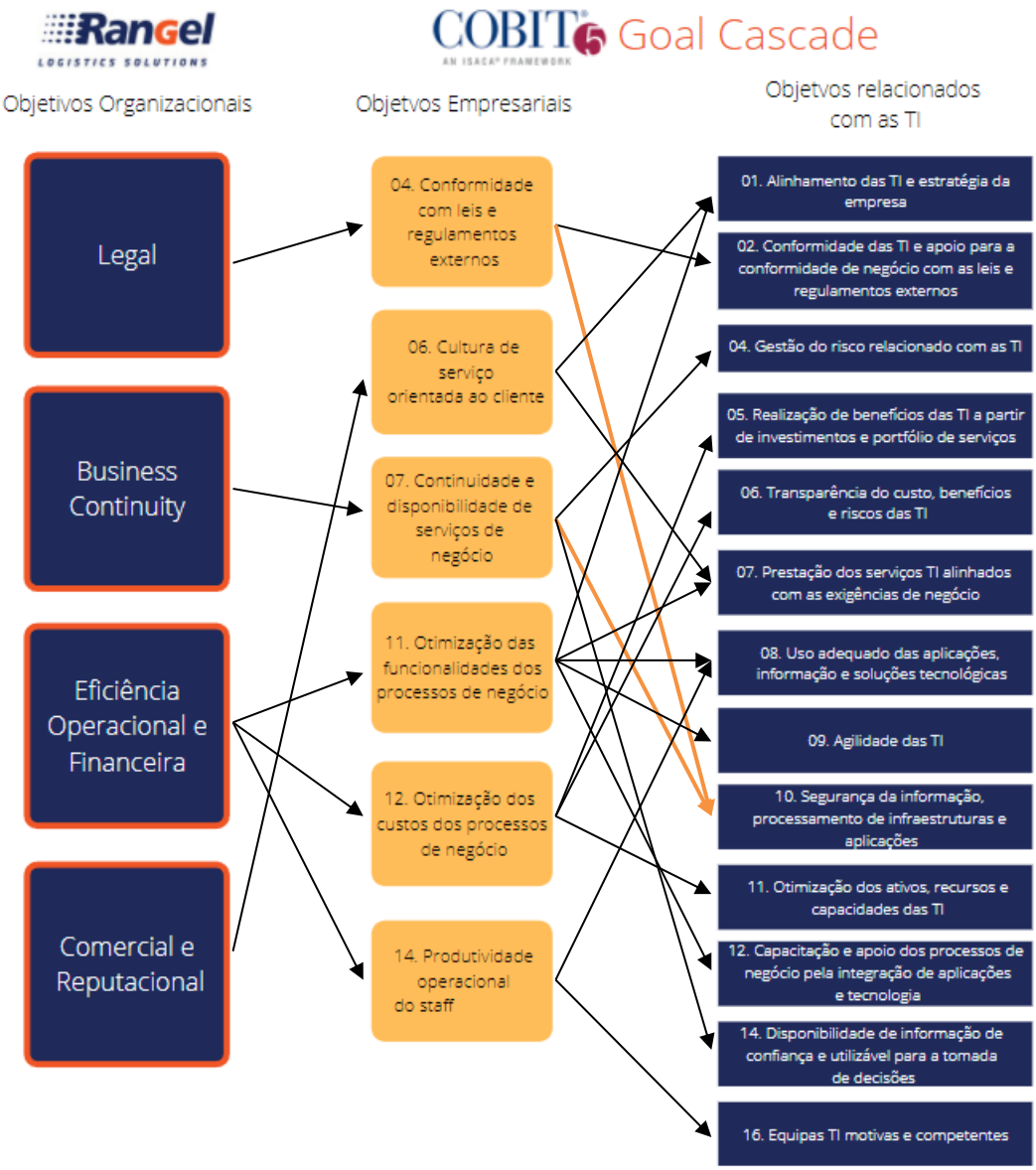


Figura 16 - Cobit 5 Goals Cascade

Por razões óbvias e visíveis neste mapeamento, é de destacar o objetivo relacionado com as TI nº10, "segurança da informação, processamento de infraestruturas e aplicações", como sendo o objeto de estudo deste projeto.

Tal como referido anteriormente, este objetivo também está mapeado a um número determinado de processos, neste caso, **5 processos**.

Nas tabelas seguintes estão identificadas as métricas do objetivo relacionado com as TI nº10 e as métricas dos objetivos empresariais do COBIT 5 a que lhe correspondem (Tabela 3) e, por fim, as métricas dos respetivos processos (Tabela 4).

Tabela 1 - Métricas dos Objetivos Empresariais e Objetivos relacionados com as TI

(ISACA, 2012)

Objetivos Empresariais	Objetivos relacionados com as TI

04. Conformidade com leis e regulamentos externos	10. Segurança da informação, processamento de infraestruturas e aplicações
• Custo de não conformidade com regulamentos, incluindo acordos e coimas • Número de problemas de não conformidade com regulamentos provocando visualização publica e publicidade negativa • Número de problemas de não conformidade com regulamentos sobre contratos com parceiros de negócio	• Número de incidentes de segurança provocando perda financeira, interrupção de negócio ou constrangimento público • Número de serviços TI com requisitos de seguranças excelentes • Tempo para conceder, alterar e remover privilégios de acesso em comparação com os serviços acordados • Frequência de avalizações à segurança segundo as últimas normas e orientações
07. Continuidade e disponibilidade de serviços de negócio	
• Número de interrupções no serviço ao cliente que provocaram incidentes • Custos de incidentes de negócio • Número de horas perdidas no processamento devido a interrupções não planeado do serviço • Percentagem de reclamações em função de objetivos de disponibilidade de serviço comprometido	

Todo este alinhamento do mecanismo do *Goal Cascade* serve de guia para identificar um estado futuro de maturidade ao nível das tecnologias da informação desejável pela empresa de forma a cumprir os objetivos a que se predispôs, explicado e descrito nos capítulos seguintes.

A tabela seguinte (Tabela 4), apresenta os **5 processos** que se relacionam com o objetivo relacionado com as TI de estudo e respetivas métricas.

Tabela 2 - Objetivos dos Processos que correspondem ao objetivo relacionado com as TI do COBIT 5 e respetivas métricas

(ISACA, 2012)

Processo: EDM03 Garantir a Otimização do Risco	
Objetivo do processo	Métricas relacionadas
1. Os limites do risco são definidos e comunicados; Riscos relacionados com as TI são conhecidos	• Nível de alinhamento entre o risco das TI e risco empresarial • Número de riscos potenciais de TI identificados e geridos • Índice de atualização do fator de avaliação do risco
2. A organização gere o risco críticos relacionados com as TI de forma eficaz e eficiente.	• Percentagem de projetos da empresa que consideram o risco das TI • Percentagem dos planos de ação do risco das TI executados no tempo

	• Percentagem de risco crítico mitigado eficazmente
3. Risco relacionado com as TI não excede	• Nível do impacto da empresa não esperado • Percentagem do risco das TI que excede a tolerância de risco
Processo: APO12 Gerir o Risco	
Objetivo do processo	Métricas relacionadas
1. O risco relacionado com as TI é identificado, gerido e reportado	• Grau de visibilidade e reconhecimento do ambiente atual • Número de eventos de perda de características chave capturadas nos repositórios • Percentagem de auditorias, eventos e tendências capturadas em repositórios
2. Existe um perfil do risco corrente e completo	• Percentagem de processos chave de negócio incluídos no perfil do risco • Completação dos atributos e valores no perfil do risco
3. Todas as ações significantes de gestão do risco são geridas e sob controle	• Percentagem de propostas de gestão de risco rejeitas devido à falta de consideração de outros riscos • Número de incidentes significantes não identificados e incluídos no portefólio de gestão do risco
4. As ações de gestão de risco são implementadas de forma eficaz	• Percentagem dos planos de ação do risco das TI executados como delineados • Número de medidas que não reduzem o risco residual
Processo: APO12 Gerir a Segurança	
Objetivo do processo	Métricas relacionadas
1. Um sistema está no plano que considera e aborda de forma eficaz os requisitos de segurança da informação da empresa	• Número de papeis relevantes de segurança definidos de forma clara • Número de incidentes de segurança
2. Um plano dessegurança foi estabelecido, aceitado e comunicado a toda a organização	• Nível de satisfação das partes interessadas com o plano de segurança em toda a organização • Número de soluções de segurança desviantes do plano • Número de soluções de segurança desviantes da arquitetura da empresa
3. Soluções de segurança da informação estão implementadas e operados consistente em toda a organização	• Número de serviços • Número de incidentes de segurança provocados pela não aderença ao plano de segurança • Número de soluções desenvolvidas com
BAI06 Gerir Mudanças	
Objetivo do processo	Métricas relacionadas

1. As alterações autorizadas são feitas em tempo útil e com o mínimo de erros	• Quantidade de retrabalho provocado por mudanças falhadas • Tempo reduzido e esforço necessário para mudanças • Número e idade pedidos de mudança em *backlog*
2. As avaliações de impacto revelam o efeito da mudança em todos componentes afetados	• Percentagem de alterações má sucedidas devido ao impacto de avaliações inadequadas.
3. Todas as alterações de emergência são revistas e autorizadas após a mudança	• Percentagem de alterações totais que são reparações de emergências • Número de alterações de emergência não autorizadas após a mudança
4. Os principais interessados são mantidos informados de todos os aspetos da mudança	• Opinião das partes interessadas sobre a satisfação com comunicações
DSS05 Gerir Serviços de Segurança	
Objetivo do processo	Métricas relacionadas
1. A segurança das redes e comunicações reúne negócios necessidades	• Número de vulnerabilidades descobertas • Número de violações de firewall
2. Informação processada, armazenada e transmitida por os dispositivos endpoint são protegidos	• Percentagem de testes periódicos de segurança ambiental dispositivos • Classificação média para avaliações de segurança física • Número de incidentes relacionados com a segurança física
3. Todos os utilizadores são identificáveis de forma única e têm direitos de acesso de acordo com o seu papel comercial	• Tempo médio entre a alteração e a atualização das contas • Número de contas (vs. número de contas autorizadas utilizadores/pessoal)
4. Foram implementadas medidas físicas para proteger informação de acesso não autorizado, danos e interferência ao ser processada, armazenada ou transmitida	• Percentagem de testes periódicos de segurança ambiental dispositivos • Classificação média para avaliações de segurança física • Número de incidentes relacionados com a segurança física
5. A informação eletrónica é devidamente protegida quando armazenada, transmitido ou destruído	• Número de incidentes relacionados com o acesso não autorizado a informação

4. Descrição e Análise do Processo

Este capítulo tem o objetivo de apresentar a realização de uma análise da área de estudo, neste caso, uma avaliação aos sistemas de informação através da estrutura de referência. Assim, procurou-se definir um modelo que permitisse aferir o nível de maturidade atual no plano da segurança da informação, de modo, que numa segunda fase fosse possível promover a evolução da mesma para níveis mais elevados. Para um melhor entendimento, não só será apresentado o nível atual de segurança das tecnologias de informação, mas também será apresentado um estado futuro da organização.

4.1 Diagnóstico da Situação Atual

Para a realização do diagnóstico do estado atual às tecnologias de informação do grupo Rangel, foi utlizada a *framework MaturityScpape – IT Security 2* delineada pela IDC, sendo identificado para cada uma das dimensões, e respetivas subdimensões, o grau de maturidade atual de segurança das TI, designado como estado AS-IS. Esta avaliação foi realizada através do método de entrevista ao diretor do DSI (Direção dos Sistemas de Informação) do grupo Rangel, e também, meu orientador na empresa, Miguel Cordeiro.

4.1.1 Análise da dimensão Visão

Primeiramente, foi efetuada a avaliação da dimensão **visão**. Para este processo, foi feito a avaliação de cada uma das suas subdimensões, sendo atribuído o grau de maturidade desta dimensão através do cálculo da média do grau de maturidade de todas as subdimensões. As subdimensões desta dimensão são:

- Objetivos de negócio
- Objetivos de segurança
- Fiscalização regulatória
- Finança/Economia

Visão	2,75	Estágios				
		(1) Ad Hoc	(2)Opportunistic	(3) Repeatable	(4) Managed	(5) Optimized
Objetivos de negócio	2					
Objetivos de segurança	4					
Fiscalização regulatória	2					
Finança/Economia	3					

Figura 17 - Estado Atual da dimensão Visão

O grau de maturidade final desta primeira dimensão analisada é 2,75, tal como é possível comprovar através da observação da *Figura 17*. Para a chegar a esta classificação, foi a realizada a média dos graus de maturidade das respetivas subdimensões, tendo a subdimensão "objetivos de negócio" o nível 2 (*Opportunistic*), a subdimensão "objetivos de segurança" o nível 4 (*Managed*), a subdimensão "fiscalização regulatória" o nível 2 (*Opportunistic*) e a subdimensão "finança/economia" o nível 3 (*Repeatable)*. Por conseguinte, obtém-se a seguinte expressão:

$$Nível\ de\ maturidade\ atual\ da\ dimensão\ Visão = \frac{2+4+2+3}{4} = 2{,}75.$$

Um nível 2 (*Opportunistic*) na subdimensão "objetivos de negócio" significa que na Rangel, as decisões TI para as iniciativas de negócio e decisões de trabalho vão ao encontro de todos os requisitos legais.

Um nível 4 (*Managed*) na subdimensão "objetivos de segurança" significa que a Rangel, procura seguir os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade dos recursos dados de informação, de modo a protegê-los contra as ameaças possíveis tendo em conta o custo dos controlos.

Um nível 2 (*Opportunistic*) na subdimensão "fiscalização regulatória" significa que a Rangel aborda os regulamentos aplicáveis quando necessário.

Um nível 3 (*Repeatable)* na subdimensão "finança/economia" significa que a Rangel cria um orçamento anual de segurança e exige uma justificação qualitativa para as despesas.

4.1.2 Análise da dimensão Gestão de Risco

De seguida, foi realizada a avaliação da dimensão **gestão de risco**. Para este processo, foi feito a avaliação de cada uma das suas subdimensões, sendo atribuído o grau de maturidade desta dimensão através do cálculo da média do grau de maturidade de todas as subdimensões. As subdimensões desta dimensão são:

- Abordagem do risco

- Metodologias/medidas
- Relações externas
- Ambiente de controlo

Gestão de Risco	**2,25**	Estágios				
		(1) Ad Hoc	(2)Opportunistic	(3) Repeatable	(4) Managed	(5) Optimized
Abordagem do risco	1					
Metodologias/medidas	4					
Relações externas	1					
Ambiente de controlo	3					

Figura 18 - Estado Atual da dimensão gestão de risco

O grau de maturidade final desta dimensão analisada é 2,25; tal como é possível comprovar através da observação da *Figura 18*. Para a chegar a esta classificação, foi a realizada a média dos graus de maturidade das respetivas subdimensões, tendo a subdimensão "abordagem do risco" o nível 1 (*Ah Hoc*), a subdimensão "metodologias/medidas" o nível 4 (*Managed),* a subdimensão "relações externas" o nível 1 (*Ah Hoc*) e a subdimensão "ambiente de controlo" o nível 3 (*Repeatable*). Por conseguinte, obtém-se a seguinte expressão:

$$Nível\ de\ maturidade\ atual\ da\ dimensão\ Gestão\ de\ Risco = \frac{1+4+1+3}{4} = 2{,}25$$

Um nível 1 (*Ad Hoc*) na subdimensão "abordagem do risco" significa que a Rangel avalia o controlo das debilidades identificadas por auditorias externas e implementa aqueles que são mais simples.

Um nível 4 (*Managed*) na subdimensão "metodologias/medidas" significa que a Rangel incorpora uma distribuição de custos financeiros, perdas e probabilidades nas decisões de gestão do risco através de programas de métricas de segurança e resultados de controlo, de foram a avaliar a eficácia.

Um nível 1 (*Ad Hoc*) na subdimensão "relações externas" significa que a Rangel aborda os requisitos de segurança de terceiros caso-a-caso.

Um nível 3 (*Repeatable*) na subdimensão "ambiente de controlo" significa que a Rangel mantém um ambiente de controlo robusto com defesa de proteção profunda focada em redes, *hosts* e algumas aplicações que esteja alinhada com uma estrutura de referência.

4.1.3 Análise da dimensão Pessoas

Depois, foi efetuada a avaliação da dimensão **pessoas**. Para este processo, foi feito a avaliação de cada uma das suas subdimensões, sendo atribuído o grau de maturidade desta dimensão através do cálculo da média do grau de maturidade de todas as subdimensões. As subdimensões desta dimensão são:

- Liderança executiva
- Cultura organizacional
- Executivos de segurança (CISO)
- Contratação de terceiros para segurança

Pessoas	**2,25**	Estágios				
		(1) Ad Hoc	(2)Opportunistic	(3) Repeatable	(4) Managed	(5) Optimized
Abordagem do risco	3					
Metodologias/medidas	2					
Relações externas	1					
Ambiente de controlo	3					

Figura 19 - Estado atual da dimensão pessoas

O grau de maturidade final desta dimensão analisada é 2,25; tal como é possível comprovar através da observação da *Figura 19*. Para a chegar a esta classificação, foi a realizada a média dos graus de maturidade das respetivas subdimensões, tendo a subdimensão "liderança executiva" o nível 3 (*Repeatable*), a subdimensão "cultura organizacional" o nível 2 (*Opportunistic*), a subdimensão "Executivos de segurança (CISO)" o nível 1 (*Ad Hoc*) e a subdimensão "Contratação de terceiros para segurança" o nível 3 (*Repeatable).* Visto isso, obtém-se a seguinte expressão:

$$Nível\ de\ maturidade\ atual\ da\ dimensão\ Pessoas\ = \frac{3+2+1+3}{4} = 2{,}25$$

Um nível 3 (*Repeatable*) na subdimensão "liderança executiva" significa que a Rangel sistematicamente, procura orientação dos executivos de segurança sobre a conformidade das atividades e orçamento dos requisitos com a expectativa de perfeita segurança.

Um nível 2 (*Opportunistic*) na subdimensão "cultura organizacional" significa que a Rangel entende as necessidades de segurança, habitualmente seguindo as políticas e participando em treino de consciencialização.

Um nível 1 (*Ad Hoc*) na subdimensão "Executivos de segurança (CISO)" significa que a Rangel apenas assegura as necessidades de segurança operacional básica.

Um nível 3 (*Repeatable*) na subdimensão "Contratação de terceiros para segurança" significa que a Rangel avalia a equipa de tempo inteiro e os serviços contratados como parte da discussão TCO (Total Cost of Ownership) sobre as necessidades de segurança.

4.1.4 Análise da dimensão Processos

Em quarto lugar, foi executada a avaliação da dimensão **processos**. Aqui, foi feito a avaliação de cada uma das suas subdimensões, sendo atribuído o grau de maturidade desta dimensão através do cálculo da média do grau de maturidade de todas as subdimensões. As subdimensões desta dimensão são:

- Gestão de confiança
- Gestão de identidade
- Gestão de vulnerabilidades
- Gestão de ameaças

Processos	**2**	Estágios				
		(1) Ad Hoc	(2)Opportunistic	(3) Repeatable	(4) Managed	(5) Optimized
Gestão de confiança	2					
Gestão de identidade	2					
Gestão de vulnerabilidades	2					
Gestão de ameaças	2					

Figura 20 - Estado atual da dimensão processos

O grau de maturidade final desta dimensão analisada é 2; tal como é possível comprovar através da observação da *Figura 20*. Para a chegar a esta classificação, foi a realizada a média dos graus de maturidade das respetivas subdimensões, tendo a subdimensão "gestão de confiança" o nível 2 (*Opportunistic*), a subdimensão "gestão de identidade" o nível 2 (*Opportunistic*), a subdimensão "gestão de vulnerabilidades" o nível 2 (*Opportunistic*), e a subdimensão "gestão de ameaças" o nível 2 (*Opportunistic*).

$$Nível\ de\ maturidade\ atual\ da\ dimensão\ Processos = \frac{2+2+2+2}{4} = 2.$$

Um nível 2 (*Opportunistic*) na subdimensão "gestão de confiança" significa que a Rangel gere um conjunto completo de políticas aceitáveis e fornece treino de acordo com os requisitos de conformidade. Um nível 2 (*Opportunistic*) na subdimensão "gestão de identidade" significa que na Rangel, os administradores de contas criam/modificam/eliminam as próprias contas que gerem, utilizando processos estandardizados e, por vezes, realizam a revisão de acessos.

Um nível 2 (*Opportunistic*) na subdimensão "gestão de vulnerabilidades" significa que a Rangel utiliza processos de atualizações para o software adquirido; periodicamente, revê as suas configurações e repara as vulnerabilidades identificadas.

Um nível 2 (*Opportunistic*) na subdimensão "gestão de ameaças" significa que a Rangel monitoriza as entradas e alertas de segurança dos recursos TI mais críticos, de forma a identificar e abordar incidentes e outros eventos relacionados com segurança. Além disso, a Rangel monitoriza-os ao longo do seu ciclo de vida para relatórios de conformidade.

4.1.5 Análise da dimensão Tecnologias de Segurança

Por fim, foi efetuada a avaliação da dimensão **tecnologias de segurança**. Para este processo, foi realizada a avaliação de cada uma das suas subdimensões, sendo atribuído o grau de maturidade desta dimensão através do cálculo da média do grau de maturidade de todas as subdimensões. As subdimensões desta dimensão são:

- Gestão de identidade
- Gestão de vulnerabilidades
- Gestão de ameaças
- Gestão de confiança

Tecnologias de segurança	**2**	Estágios				
		(1) Ad Hoc	(2)Opportunistic	(3) Repeatable	(4) Managed	(5) Optimized
Gestão de identidade	2					
Gestão de vulnerabilidades	2					
Gestão de ameaças	3					
Gestão de confiança	1					

Figura 21 - Estado atual da dimensão tecnologias de segurança

O grau de maturidade final desta dimensão analisada é 2, tal como é possível comprovar através da observação da *Figura 21*. Para a chegar a esta classificação, foi a realizada a média dos graus de maturidade das respetivas subdimensões, tendo a subdimensão "gestão de identidade" o nível 2 (*Opportunistic*), a subdimensão "gestão de vulnerabilidades" o nível 2 (*Opportunistic*), a subdimensão "gestão de ameaças" o nível 3 (*Repeatable*) e a subdimensão "gestão de confiança" o nível 1 (*Ad Hoc*). Visto isso,

$$Nível\ de\ maturidade\ da\ dimensão\ Tecnologias\ de\ Segurança = \frac{2+2+3+1}{4} = 2.$$

Um nível 2 (*Opportunistic*) na subdimensão "gestão de identidade" significa que a Rangel impulsiona palavras-chave seguras e entradas únicas para todos os recursos. Também utiliza autenticação multi-fator para acessos à distância, acessos privilegiados e acessos para terceiros.

Um nível 2 (*Opportunistic*) na subdimensão "gestão de vulnerabilidades" significa que a Rangel utiliza *firewalls* de camada de redes com identificação e consciência de aplicação para filtragens e separação de redes.

Um nível 3 (*Repeatable*) na subdimensão "gestão de ameaças" significa que a Rangel deteta ameaças usando assinaturas, detonação sandbox, heurísticas nas redes e *endpoints,* e incorpora deteção da capacidade de violações nos dados e aplicações.

Um nível 1 (*Ad Hoc*) na subdimensão "gestão de confiança" significa que a Rangel emprega comunicações encriptadas *ad hoc.*

4.1.6 Nível Global de Maturidade do Estado Atual

Depois de estabelecer um nível de maturidade para cada uma das cinco dimensões, descritos nos subcapítulos anteriores, pelo mesmo método que se determinou o nível dessas subdimensões, também foi possível determinar o nível de maturidade global do estado atual de segurança. Para tal, através do nível atribuído a cada uma subdimensão, realizou-se a média dos mesmos. Por conseguinte, obtém-se a seguinte expressão:

$$Nível\ global = \frac{2{,}75 + 2{,}25 + 2{,}25 + 2 + 2}{5} = 2{,}25$$

Assim, conclui-se que o nível de maturidade global do estado atual é de 2,25; como se pode observar na *Figura 22*, atribuindo, desta forma, o nível Opportunistic, porém já com processos de melhoria englobados no nível 3 (Repeatable).

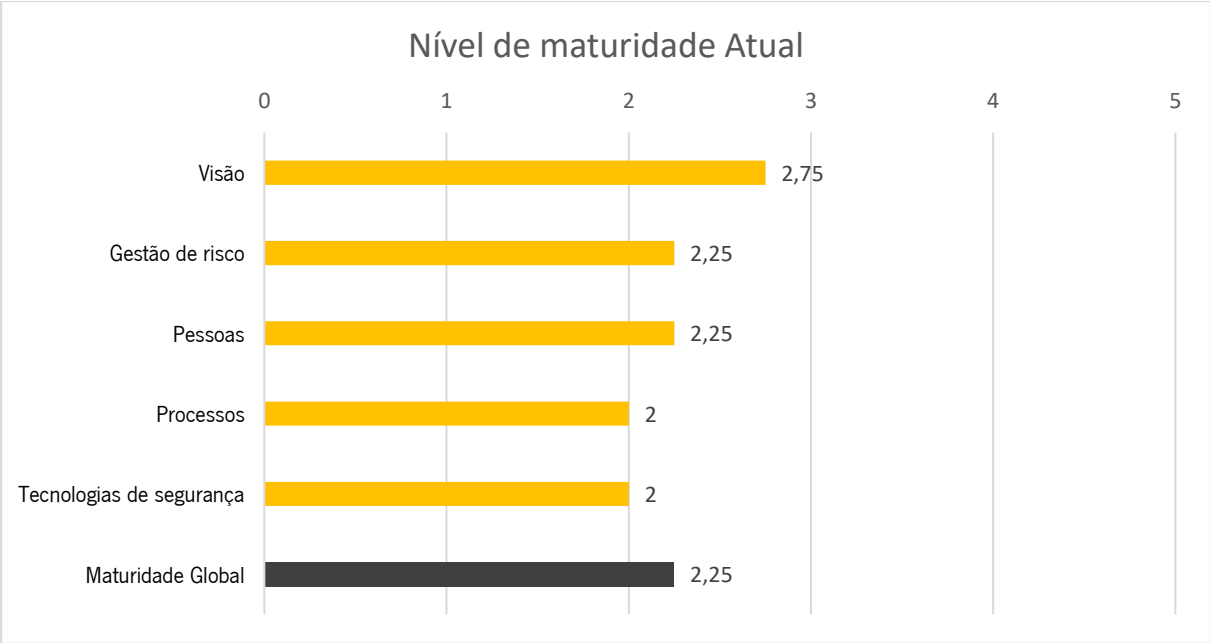


Figura 22 - Nível global de maturidade do estado atual

5. Oportunidades de Melhoria e Análise do Estado Futuro

Neste capítulo, serão apresentadas as oportunidades de melhoria levantadas no processo de análise ao estado atual das tecnologias de informação, e respetivas iniciativas que foram desenvolvidas no âmbito do projeto de investigação.

5.1 Oportunidades de Melhoria

No capítulo 3, foi apresentado o alinhamento dos objetivos organizacionais com os objetivos TI segundo os objetivos da estrutura de referência COBIT. Tendo em conta esse alinhamento estratégico, na fase de diagnóstico das tecnologias de informação, denominado de fase AS-IS, foi possível reportar falhas e situações que podem justificar uma ação, sendo assim, identificadas oportunidades de melhoria.

Depois da análise do estado atual das tecnologias de informação às 5 dimensões, determinou-se que existem **12 oportunidades de melhoria** (*Tabela 3*).

Tabela 3 - Oportunidades de melhoria do estado atual

Código Oportunidade de melhoria	Descrição
OM. 01	Não existe uma abordagem á gestão pelo risco no desenho das soluções de TI para suportar as iniciativas de negócio
OM. 02	Não existem práticas de auditorias internas por forma a antecipar problemas de conformidade
OM. 03	Não existe a prática da qualificação dos projetos de investimento
OM. 04	Não há avaliação à segurança de informação dos parceiros externos
OM. 05	Não existe consideração pelos requisitos de segurança de informação aquando da realização de contratos com os parceiros externos
OM. 06	Não existe uma cultura de participação ativa nos temas de segurança de informação
OM. 07	Não existe um processo de gestão de identidades e acessos aprimorado na organização
OM. 08	Não existe uma política gestão de atualizações alargada a todos os níveis da arquitetura das redes dos sistemas de informação
OM. 09	Não existe uma prática de segurança *by design* no processo de desenvolvimento de software
OM. 10	Não existem práticas de gestão de problemas (*problem management*)
OM. 11	Não existe monitorização das atividades de utilizadores privilegiados
OM. 12	Não existe uma solução avançada de segurança ao nível das redes, aplicações e *endpoints*

5.2 Análise do Estado Futuro

Após a identificação das oportunidades de melhoria, é esperado que estas sirvam de base para estabelecer um estado ótimo de maturidade das tecnologias de informação, desejado pela administração do Grupo Rangel. Para esse processo, recorreu-se novamente à estrutura de referência *IDC Maturityscape – IT Security 2.0*, pelo que, estabeleceu-se assim, novos níveis para cada dimensão e respetivas subdimensões, obtendo, desta forma, um novo estado futuro para a organização relativamente, à segurança das TI. Este novo estado designa-se por estado TO-BE.

5.2.1 Análise da dimensão Visão

Tal como no processo de análise anterior, primeiramente, foi efetuada a avaliação da dimensão **visão**. Em contraste, desta vez, a análise é realizada ao estado desta dimensão, já com as oportunidades de melhoria implementadas.

Para este processo, também foi feito a avaliação de cada uma das suas subdimensões, sendo atribuído o grau de maturidade desta dimensão através do cálculo da média do grau de maturidade de todas as subdimensões. As subdimensões desta dimensão são:

- Objetivos de negócio
- Objetivos de segurança
- Fiscalização regulatória
- Finança/Economia

Visão	**4**	Estágios				
		(1) Ad Hoc	(2)Opportunistic	(3) Repeatable	(4) Managed	(5) Optimized
Objetivos de negócio	4					
Objetivos de segurança	4					
Fiscalização regulatória	4					
Finança/Economia	4					

Figura 23 – Estado Futuro da dimensão Visão

Relativamente ao estado futuro, o grau de maturidade final desta primeira dimensão analisada é 4, tal como é possível comprovar através da observação da *Figura 23*. Esta classificação obtém-se pela realização da média dos graus de maturidade das respetivas subdimensões, tendo a subdimensão "objetivos de negócio" o nível 4 (*Managed*), a subdimensão "objetivos de segurança" o nível 4 (*Managed*), a

subdimensão "fiscalização regulatória" o nível 4 (*Managed*) e a subdimensão "finança/economia" o nível 4 (*Managed*), representado na seguinte expressão:

$$Nível\ de\ maturidade\ da\ dimensão\ Visão = \frac{4+4+4+4}{4} = 4$$

Um nível 4 (*Managed*) na subdimensão "objetivos de negócio" significa que a Rangel integra estimativas de probabilidade e perdas juntamente com controlo de custos ao alinhar as necessidades TI para as iniciativas de negócio.

Para a subdimensão "objetivos de segurança", o nível de maturidade mantém-se, ou seja, mantém o nível 4 (*Managed*), o que significa que a Rangel procura seguir os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade dos recursos dados de informação, de modo a protegê-los contra as ameaças possíveis tendo em conta o custo dos controlos.

Um nível4 (*Managed*) na subdimensão "fiscalização regulatória" significa que a Rangel mantém um programa detalhado, pelo qual, a conformidade regulatória é assegurada através de iniciativas pró-ativas.

Relativamente à subdimensão "finança/economia, um nível 4 (Managed), quer dizer que a Rangel realiza uma conduta quantitativa de uma análise custo-benefício, no que diz respeito a projetos de segurança.

5.2.2 Análise da dimensão Gestão de Risco

De seguida, também foi realizada a avaliação da dimensão **gestão de risco**. Desta vez, a análise é realizada ao estado desta dimensão, já com as oportunidades de melhoria implementadas. Tal como para o diagnóstico do estado atual, para este processo, foi feito a avaliação de cada uma das suas subdimensões, sendo atribuído o grau de maturidade desta dimensão através do cálculo da média do grau de maturidade de todas as subdimensões. As subdimensões desta dimensão são:

- Abordagem do risco
- Metodologias/medidas
- Relações externas
- Ambiente de controlo

Gestão de Risco	3,75	Estágios				
		(1) Ad Hoc	(2)Opportunistic	(3) Repeatable	(4) Managed	(5) Optimized
Abordagem do risco	4					
Metodologias/medidas	4					
Relações externas	3					
Ambiente de controlo	4					

Figura 24 - Estado Futuro da dimensão Gestão de Risco

Para esta dimensão analisada, no que diz respeito ao estado futuro, o grau de maturidade final é 3,75; tal como a *Figura 24* comprova. Esta classificação obtém-se pela realização da média dos graus de maturidade das respetivas subdimensões, tendo a subdimensão "Abordagem do risco" o nível 4 (*Managed*), a subdimensão "Metodologias/medidas" o nível 4 (*Managed*), a subdimensão "Relações externas" o nível 3 (*Repeatable*) e a subdimensão "Ambiente de controlo" o nível 4 (*Managed*), representado na seguinte expressão:

$$Nível\ de\ maturidade\ da\ dimensão\ Gestão\ de\ Risco = \frac{4+4+3+4}{4} = 3{,}75$$

Para a subdimensão "Abordagem do risco", atribuiu-se um nível 4 (*Managed*), o que significa que a Rangel conduz análises custo-serviço, pelo que, procura o ponto ótimo de "risco reduzido por custo de unidade", relativamente aos projetos de segurança TI.

Atribuir um nível 4 (M*anaged*) na subdimensão "Metodologias/medidas", significa que a Rangel incorpora uma distribuição de custos financeiros, perdas e probabilidades em função das decisões da gestão de risco, usando métricas de programas de segurança e resultados de controlo para avaliar a eficácia.

Relativamente à subdimensão "Relações externas", atribuir um nível 3 (*Repeatable*) quer dizer que a Rangel incorpora requisitos de segurança de TI nos contratos e conduz algumas auditorias de diligência, obtém auditorias externas e certificações para parceiros.

Atribuir um nível 4 (*Managed*) na subdimensão "Ambiente de controlo", significa que a Rangel emprega seletivamente controlos granulares oportunos em ambientes físicos e ambientes cibernéticos com base numa estrutura de referência de controlos.

5.2.3 Análise da dimensão Pessoas

A terceira dimensão avaliada no estado futuro foi a dimensão **pessoas**. Em contraste, desta vez, a análise é realizada ao estado desta dimensão, já com as oportunidades de melhoria implementadas.

Para este processo, também foi feito a avaliação de cada uma das suas subdimensões, sendo atribuído o grau de maturidade desta dimensão através do cálculo da média do grau de maturidade de todas as subdimensões. As subdimensões desta dimensão são:

- Liderança executiva
- Cultura organizacional
- Executivos de segurança (CISO)
- Contratação de terceiros para segurança

Pessoas	**3,5**	Estágios				
		(1) Ad Hoc	(2)Opportunistic	(3) Repeatable	(4) Managed	(5) Optimized
Abordagem do risco	4					
Metodologias/medidas	3					
Relações externas	4					
Ambiente de controlo	3					

Figura 25 - Estado Futuro da dimensão Pessoas

Relativamente ao estado futuro desta dimensão, o grau de maturidade final é 3,5; tal como é possível comprovar através da observação da *Figura 25*. Esta classificação obtém-se pela realização da média dos graus de maturidade das respetivas subdimensões, sendo atribuído à subdimensão "Liderança Executiva" o nível 4 (*Managed*), à subdimensão "Cultura organizacional" o nível 3 (*Repeatable*), à subdimensão "Executivos de segurança (CISO)" o nível 4 (*Managed*) e, por fim, é atribuído à subdimensão "Contratação de terceiros para segurança" o nível 3 (*Repeatable*), representado na seguinte expressão:

$$Nível\ de\ maturidade\ da\ dimensão\ Pessoas = \frac{4+3+4+3}{4} = 3{,}5$$

A classificação de nível 4 (*Managed*) na subdimensão "Liderança Executiva" significa que a Rangel convida os executivos de segurança para a reuniões da administração geral e ativamente promove o seu envolvimento em avaliações de risco de tecnologias e custos de controlos como parte de decisões de TI. (reescrever isto a amarelo)

Para a subdimensão "Cultura organizacional", um nível 3 (*Repeatable*) significa que a Rangel frequentemente notifica o departamento de segurança sobre todas as preocupações/dúvidas de segurança.

Um nível 4 (*Managed*) na subdimensão "Executivos de segurança (CISO)" significa que a Rangel mantém os administradores informados sobre os indicadores de risco para toda a atividade TI e estes participam decisões de negócio aplicáveis às TI.

Para a subdimensão "Contratação de terceiros para segurança", o nível de maturidade mantém-se, ou seja, mantém o nível 3 (*Repeatable*) quer dizer que a Rangel tem um foco providenciar todas as necessidades do staff de segurança, aumentar os contratos de longo prazo e gerir os serviços de segurança quando aplicáveis ou necessários.

5.2.4 Análise da dimensão Processos

A seguir, também foi realizada a avaliação da dimensão **processos**. Desta vez, a análise é realizada ao estado futuro desta dimensão, assumindo que as oportunidades de melhoria foram suprimidas. Tal como para o diagnóstico do estado atual, para este processo, foi feito a avaliação de cada uma das suas subdimensões, sendo atribuído o grau de maturidade desta dimensão através do cálculo da média do grau de maturidade de todas as subdimensões. As subdimensões desta dimensão são:

- Gestão de confiança
- Gestão de identidade
- Gestão de vulnerabilidades
- Gestão de ameaças

Processos	**4**	Estágios				
		(1) Ad Hoc	(2)Opportunistic	(3) Repeatable	(4) Managed	(5) Optimized
Gestão de confiança	4					
Gestão de identidade	5					
Gestão de vulnerabilidades	4					
Gestão de ameaças	3					

Figura 26 - Estado Futuro da dimensão Processos

Para esta dimensão analisada, no que diz respeito ao estado futuro, o grau de maturidade final é 4, tal como a *Figura 26* comprova. Esta classificação obtém-se pela realização da média dos graus de maturidade das respetivas subdimensões, tendo a subdimensão "Gestão de confiança" o nível 4 (*Managed*), a subdimensão "Gestão de identidade" o nível 5 (*Optimized*), a subdimensão "Gestão de vulnerabilidades" o nível 4 (*Managed*) e a subdimensão "Gestão de ameaças" o nível 3 (*Repeatable*), representado na seguinte expressão:

$$Nível\ de\ maturidade\ da\ dimensão\ Visão = \frac{4+5+4+3}{4} = 4$$

Para a subdimensão "Gestão de confiança", atribuiu-se um nível 4 (*Managed*), o que significa que a Rangel toma decisões baseadas na gestão de políticas e revisão de atividades que encontram provas de eficácia.

Atribuir um nível 5 (*Optimized*) na subdimensão "Gestão de identidade", significa que a Rangel emprega uma filosofia de privilégios mínimos, de modo, a gerir os utilizadores num contexto de total perceção das suas credenciais, acessos e atividades.

Relativamente à subdimensão "Gestão de vulnerabilidades", atribuir um nível 4 (*Managed*) quer dizer que a Rangel avalia a relação custo-eficácia do sistema de configurações e atualizações; e integra na sua plenitude atividades de aplicação de níveis de segurança no desenvolvimento de processos.

Atribuir um nível 3 (*Repeatable*) na subdimensão "Gestão de ameaças", significa que a Rangel executa uma monitorização de alertas e eventos 24X7 em todo o ambiente TI, responde com base numa análise causa-raiz dos recursos afetados e notifica de acordo a situação.

5.2.5 Análise da dimensão Tecnologias de Segurança

A última dimensão avaliada no estado futuro foi a dimensão **tecnologias de segurança**. Em contraste, desta vez, a análise é realizada ao estado futuro desta dimensão, já com as oportunidades de melhoria suprimidas.

Para este processo, também foi feito a avaliação de cada uma das suas subdimensões, sendo atribuído o grau de maturidade desta dimensão através do cálculo da média do grau de maturidade de todas as subdimensões. As subdimensões desta dimensão são:

- Gestão de identidade
- Gestão de vulnerabilidades
- Gestão de ameaças
- Gestão de confiança

Tecnologias de segurança	**3**	Estágios				
		(1) Ad Hoc	(2)Opportunistic	(3) Repeatable	(4) Managed	(5) Optimized
Gestão de identidade	2					
Gestão de vulnerabilidades	4					
Gestão de ameaças	4					
Gestão de confiança	2					

Figura 27 - Estado Futuro da dimensão Tecnologias de Segurança

Relativamente ao estado futuro desta dimensão, o grau de maturidade final é 3; tal como é possível comprovar através da observação da *Figura 27*. Esta classificação obtém-se pela realização da média dos graus de maturidade das respetivas subdimensões, sendo atribuído à subdimensão "Gestão de identidade" o nível 2 (*Opportunistic*), à subdimensão "Gestão de vulnerabilidades" o nível 4 (*Managed*), à subdimensão "Gestão de ameaças" o nível 4 (*Managed*) e, por fim, é atribuído à subdimensão "Gestão de confiança" o nível 2 (*Opportunistic*), representado na seguinte expressão:

$$Nível\ de\ maturidade\ da\ dimensão\ Visão = \frac{2+4+4+2}{4} = 3$$

Para a subdimensão "Gestão de identidade", o nível de maturidade mantém-se, ou seja, mantém o nível 2 (*Opportunistic*) quer dizer que a Rangel impulsiona palavras-chave seguras e entradas únicas para todos os recursos. Também utiliza autenticação multi-fator para acessos à distância, acessos privilegiados e acessos para terceiros.

Um nível 4 (*Managed*) na subdimensão "Gestão de vulnerabilidades" significa que a Rangel utiliza *firewalls* de multiníveis e *proxies* em todas as redes e emprega técnicas de isolamento de carga de trabalho (como por exemplo, *virtual machines*)

Para a subdimensão "Gestão de ameaças", um nível 4 (*Managed*) significa que a Rangel deteta ameaças usando assinaturas, detonação *sandbox*, deteção de anomalias e *machine learning* nas redes e nas atividades do sistema. Além disso, identifica dados sensíveis serem transmitidos para o exterior.

Um nível 2 (*Opportunistic)* na subdimensão "Gestão de confiança" significa que a Rangel possui comunicações encriptadas e armazenagem *endpoint* (disco completo), além de implementar um sistema de gestão central.

5.2.6 Nível Global de Maturidade do Estado Atual

Depois de estabelecer um nível de maturidade para cada uma das cinco dimensões, descritos nos subcapítulos anteriores, pelo mesmo método que se determinou o nível dessas subdimensões, também foi possível determinar o nível de maturidade global do estado futuro de segurança. Para tal, através do nível atribuído a cada uma subdimensão, realizou-se a média dos mesmos. Por conseguinte, obtém-se a seguinte expressão:

$$\text{Nível de maturidade global do estado futuro} = \frac{4+3{,}75+3{,}5+4+3}{5} = 3{,}65$$

Assim, conclui-se que o nível de maturidade global do estado atual é de 3,65; como se pode observar na *Figura 28*, atribuindo, desta forma, o nível *Repeatable*, porém já com processos de melhoria englobados no nível 4 (*Managed*).

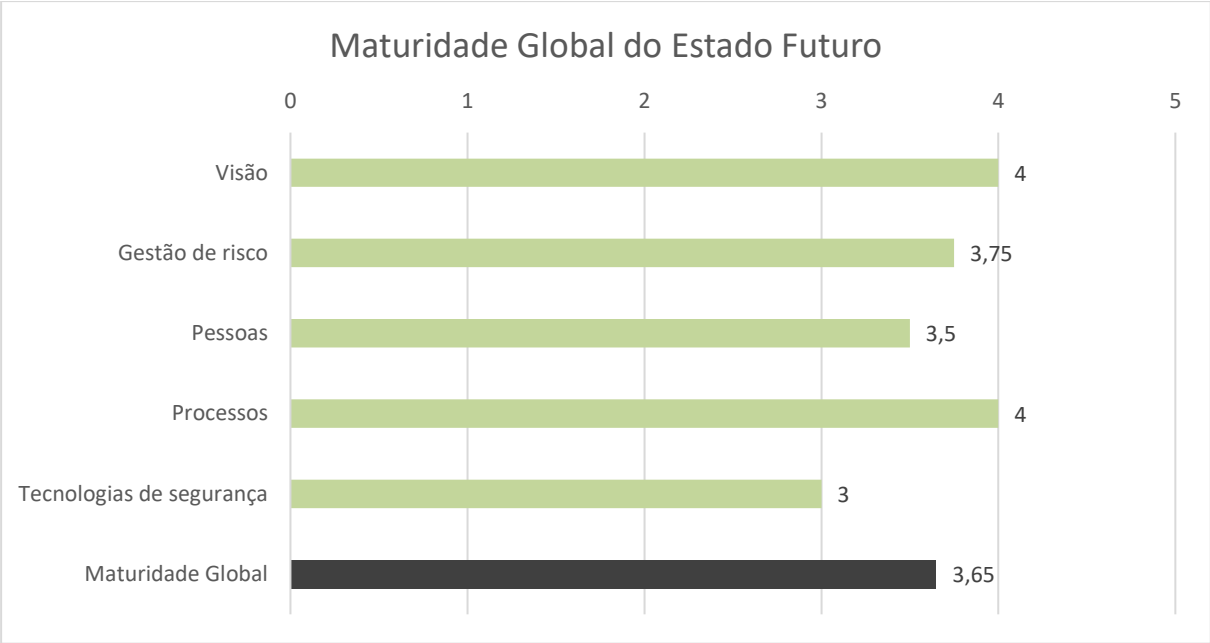


Figura 28 - Nível global de maturidade do estado futuro

6. INICIATIVAS

Neste capítulo serão apresentadas as várias iniciativas que foram criadas para alcançar o estado de maturidade futuro, no que diz respeito à segurança das tecnologias de informação. Estas iniciativas irão ingressar uma ou mais oportunidades de melhoria e, por conseguinte, ajudar a atingir este novo estado de maturidade a partir do estado atual. Com esse intuito, foi criado um total de **11 iniciativas**, que correspondem a projetos que possuem um conjunto de ações de alto nível que irão cobrir um ou mais objetivos organizacionais.

Entre os 4 objetivos organizacionais descritos na secção 3.6, apenas foram considerados os objetivos: *Bussiness Continuity*, Legal, Eficiência Operacional e Financeira. Posto isto, o objetivo organizacional **Comercial e Reputacional** não foi considerado, visto que, não tem diretamente ligado a si uma iniciativa, ou seja, o sucesso deste objetivo tem como origem o sucesso de iniciativas ligados a outros objetivos organizacionais. O seu sucesso é uma consequência do sucesso dos outros três objetivos.

Tabela 4 – Objetivos organizacionais do grupo Rangel

Cód. Objetivo Organizacional	Descrição do Objetivo Organizacional
OO.1	Legal/Regulatório
OO.2	*Business Continuity Plan*
OO.3	Performance Operacional e Financeira

6.1 Iniciativa nº1 - Promover a Segurança de Informação na Organização

A grande importância desta iniciativa deve-se ao facto de demonstrar o posicionamento estratégico da Rangel sobre o tema de segurança da informação e os principais agentes, que são a Gestão de Topo (neste caso, a Administração do Grupo Rangel) e as Direções Corporativas. Além disto, esta iniciativa traça a linhas de orientação para toda a organização, como também acaba por cobrir logo grande parte dos requisitos para obter conformidade com o RGPD. Assim, é de esperar que se obtenha:

- A política de segurança da informação. Uma versão final que irá ser registada e transmitida para todos os colaboradores da organização. Anexada a esta política, irão ser redigidas outras versões, como por exemplo a política de segurança para os parceiros externos, entre outras que irão ser apresentadas nas iniciativas seguintes;
- Desenvolver o plano atual de comunicação com todas as partes interessadas, internas e externas, apresentado desta forma um modelo oficial de comunicação;
- A missão da rangel no tema segurança da informação e os objetivos organizacionais que pretende alcançar;

Tabela 5 - Ações da Iniciativa nº1 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	Processo ITIL	RGPD
1	Refletir sobre o contexto da organização	R.4.1	Compreender a organização e o seu contexto		Art. 24
		R.4.2	Compreender as necessidades e expectativas das partes interessadas		Art. 24
		R.4.3	Determinar o âmbito do sistema de gestão de segurança da informação		Art. 24
2	Definir e aprovar a Política de segurança da informação	R.5.2	Política		Art. 5, Art. 24
		A.5.1.1	Políticas para a segurança da informação		
3	Definir os objetivos para a segurança de informação suportado numa avaliação de risco	R.6.1.1	Generalidades		Art. 25, Art. 83, Art. 84, Art. 85, Art. 86, Art. 87, Art. 88, Art. 89, Art. 90
		R.6.1.2	Avaliação do risco de segurança da informação		Art. 5, Art. 6, Art. 7, Art. 10, Art. 11, Art. 17, Art. 18, Art. 19, Art. 20, Art. 21, Art. 22, Art. 24, Art. 25, Art. 35, Art. 36, Art. 83, Art. 84, Art. 85, Art. 86, Art. 87, Art. 88, Art. 89, Art. 90
		R.6.2	Objetivos de segurança da informação e planeamento para os alcançar		Art. 24, Art. 25, Art. 83, Art. 84, Art. 85, Art. 86, Art. 87, Art. 88, Art. 89, Art. 90

6.2 Iniciativa nº2 - Modelo de Governança

Esta iniciativa tem como objetivo definir e estabelecer um modelo de governança para a segurança da informação. Através de iniciativas de vontade própria e por motivos organizacionais e funcionais de trabalho, a Rangel já apresenta uma definição estruturação de responsabilidades de segurança da

informação, apesar de não completo para todas campos na área. Visto isto, para implementar esta iniciativa deve-se:

- Definir e projetar o sistema de gestão de segurança da informação;
- Uma vez que a Rangel já possui um Sistema de Gestão da Qualidade (SGQ), é necessário avaliar os contributos da ISO 9001:2015 para o SGSI, de forma a poder integrá-lo no existente sistema;
- Estabelecer relacionamentos de interesse e meios de comunicação com esses mesmo grupos de interesse, como entidades externas, autoridades, entidades reguladoras, etc. Exemplo: Centro nacional de Proteção de Dados (CNPD), Centro Nacional de Cibersegurança (CNCS);
- Desenvolver um plano de comunicação que garanta o contato permanente entre a equipa interna, os seus congéneres nos subcontratados e a entidade de controlo (CNPD)

Tabela 6 - Ações da Iniciativa nº2 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	Processo ITIL	RGPD
1	Implementar um Sistema de Gestão de Risco para a Segurança de Informação	R.8.1	Planeamento e controlo operacional	Gestão do risco	Art. 24
		R.8.2	Avaliação de risco de segurança da informação		Art. 24, Art. 28, Art. 32
		R.8.3	Tratamento do risco de segurança da informação		Art. 24, Art. 30
2	Definir sistemas de gestão de segurança da informação e integrar no atual sistema da qualidade (SGQ)	R.4.4	Sistema de gestão de segurança da informação		Art. 24
		R.7.5.1	Generalidades		Art. 24, Art. 27, Art. 30
		R.7.5.2	Criação e atualização		Art. 24, Art. 30
		R.7.5.3	Controlo da Informação documentada		Art. 24, Art. 30
		R.8.1	Planeamento e controlo operacional		Art. 24
		R.9.3	Revisão pela gestão		Art. 24
		R.10.1	Não conformidade e ação corretiva		Art. 24
		R.10.2	Melhoria contínua		Art. 24
		A.5.1.1	Políticas para a segurança da informação		
		A.5.1.2	Revisão das políticas para a segurança da informação		
3		R.7.4	Comunicação		Art. 24

	Estabelecer canais de comunicação com entidades competentes e grupos de interesse	A.6.1.3	Contacto com autoridades competentes		Art.31, Art. 35, Art. 36
		A.6.1.4	Contacto com grupos de interesse		

6.3 Iniciativa nº3 - Reavaliar a Metodologia de Gestão de Projetos

A Rangel é uma organização que adotou uma filosofia vocacionada para soluções de forma a satisfazer as necessidades dos seus clientes e parceiros. Consequentemente, adotou uma metodologia de gestão de projetos. Tendo em consideração as exigências de segurança da informação, a metodologia de gestão de projetos deve passar a considerar:

- No ponto de vista financeiro a qualificação dos projetos deve-se essencialmente à decisão Go – NoGo baseado no retorno de investimento;
- A tomada de decisão deve ser suportada por uma gestão e análise do risco, devendo incluir controlos dos riscos na vertente financeira, implementação e execução de projetos;

Tabela 7 - Ações da Iniciativa nº3 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	Processo ITIL	RGPD
1	Integrar no processo de decisão a gestão do risco	R.6.1.1	Generalidades	Gestão do risco	Art. 25, Art. 83, Art. 84, Art. 85, Art. 86, Art. 87, Art. 88, Art. 89, Art. 90
		R.6.1.2	Avaliação do risco de segurança da informação		Art. 5, Art. 6, Art. 7, Art. 10, Art. 11, Art. 17, Art. 18, Art. 19, Art. 20, Art. 21, Art. 22, Art. 24, Art. 25, Art. 35, Art. 36, Art. 83, Art. 84, Art. 85, Art. 86, Art. 87, Art. 88, Art. 89, Art. 90
		R.6.1.3	Tratamento do risco de segurança da informação		Art. 25, Art. 83, Art. 84, Art. 85, Art. 86, Art. 87, Art. 88, Art. 89, Art. 90

		R.8.2	Avaliação do risco de segurança da informação		Art. 24, Art. 28, Art. 32
2	Ingressar a segurança da informação na gestão de projetos	R.6.1.1	Generalidades	Gestão da segurança da informação	Art. 24, Art. 25, Art. 83, Art. 84, Art. 85, Art. 86, Art. 87, Art. 88, Art. 89, Art. 90
		R.6.1.2	Avaliação do risco de segurança da informação		Art. 5, Art. 6, Art. 7, Art. 10, Art. 11, Art. 17, Art. 18, Art. 19, Art. 20, Art. 21, Art. 22, Art. 24, Art. 25, Art. 35, Art. 36, Art. 83, Art. 84, Art. 85, Art. 86, Art. 87, Art. 88, Art. 89, Art. 90
		R.6.1.3	Tratamento do risco de segurança da informação		Art. 24, Art. 25, Art. 83, Art. 84, Art. 85, Art. 86, Art. 87, Art. 88, Art. 89, Art. 90
		A.6.1.5	Segurança da informação na gestão de projeto		
3	Introduzir a prática de qualificação financeira na gestão de projetos			Gestão financeira	

6.4 Iniciativa nº4 - Implementar Práticas de Auditorias Internas

O SGSI não é exceção da regra de que todos os sistemas de gestão são munidos de sistemas de auditoria e verificação dos controlos implementados. Assim, com esta iniciativa é esperado a implementação de um sistema de auditoria interna. Visto isto, é preciso ter em consideração os seguintes aspetos:

- Apesar da organização já possuir uma distribuição de responsabilidades para vários controlos de implementação, é preciso adicionar uma atribuição de responsabilidades relativamente a sistemas de auditoria interna;

- Possuir à disposição, recursos apropriados para a execução dos processos de auditoria;
- Analisar os contributos do sistema atual de qualidade SGQ;

Tabela 8 - Ações da Iniciativa nº4 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	Processo ITIL	RGPD
1	Projetar a implementação de processos de auditoria interna	R.9.2	Auditoria interna		Art. 24
		A.12.7.1	Controlos de auditoria e nos sistemas de informação		

6.5 Iniciativa nº5 - Relação com Terceiros

Como produto da iniciativa nº1, temos um modelo de comunicação com as partes interessadas externas da organização. Por isso, de modo a pôr em prática esse plano, é necessário definir políticas que assegurarão as medidas implementadas pelo SGSI que suportarão a relação com as entidades externas. Consequente, com esta iniciativa é de esperar os seguintes resultados:

- Uma política de segurança da informação para as partes interessadas externas da organização, que não só descreve a posição da Rangel em relação à segurança da informação, mas também, como essas entidades se devem comportar com a Rangel;
- Uma política de controlo do modo como a informação é transferida com parceiros externos, onde devem ser explícitos os seguintes pontos:
    - Transferência de dados pessoais na subcontratação de serviços;
    - Política de segurança na implementação de interfaces de sistemas de informação, para a prestação dos serviços de logística e transporte;
- Um plano de revisão dos contratos com fornecedores e prestadores de serviços, de modo a incluir cláusulas em relação à segurança da informação;

Tabela 9 - Ações da Iniciativa nº5 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	Processo ITIL	RGPD
1	Redigir uma política de segurança de informação para os parceiros externos com a inclusão de	R.7.4	Comunicação	Gestão de fornecedores	Art. 24
		A.7.1	Antes da relação contratual		Art. 10
		A.7.2.1	Responsabilidade da gestão		
		A.13.1.2	Segurança de serviços de rede		Art. 20

	cláusulas nos contratos	A.15.1	Segurança da informação nas relações com fornecedores		Art. 5, Art. 26, Art. 27, Art. 28
		A.15.2	Gestão da entrega de serviços pelos fornecedores		Art. 5, Art. 26, Art. 27, Art. 28
2	Criar uma política de transferência de informação	A.13.2.1	Políticas e procedimentos de transferência de informação		Art. 5, Art. 7, Art. 15, Art. 20, Art. 26
		A.13.2.2	Acordos sobre a transferência de informação		Art. 5, Art. 7, Art. 20, Art. 26
		A.13.2.3	Mensagens eletrónicas		Art. 5, Art. 7, Art. 20, Art. 26
		A.13.2.4	Acordos de confidencialidade ou de não divulgação		Art. 5, Art. 7, Art. 20, Art. 26

6.6 Iniciativa nº6 - Programa de Consciencialização para a Segurança da Informação

Como referido várias vezes este documento, a dimensão humana é maior vulnerabilidade dentro duma organização em relação à segurança da informação. Visto isto, esta iniciativa exige alguma importância, uma vez que visa abordar a componente do comportamento humano. Assim, as ações desta iniciativa devem assegurar uma gestão do conhecimento através da introdução de boas práticas no que diz respeito à segurança da informação.

- Aquando da integração de um novo colaborador na organização, providenciar formação na política e boas práticas, incluindo o transporte e transferência de dados para fora da organização;
- Ações de avaliação do conhecimento e consciencialização dos colaboradores para com o tema, para além de ações como simulacros de ataques e outros incidentes, campanhas de informação e treino;
- Conhecimento em geral e conhecimento sobre novas ameaças devem ser periodicamente assegurados;
- Realizar um simulacro para testar, em termos operacionais, a boa adoção dos procedimentos indicados nas alíneas anteriores;

Tabela 10 - Ações da Iniciativa nº6 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	Processo ITIL	RGPD
1	Planos de integração dos colaboradores	R.7.1	Recursos		Art. 24
		R.7.2	Competência		Art. 24
		A.7.2.2	Consciencialização, educação e formação em segurança da informação		
		A.9.3.1	Utilização da informação secreta para autenticação		Art. 16, Art. 17
2	Simulação de ataques de *phising*	R.7.3	Consciencialização		Art. 24
		A.7.2.2	Consciencialização, educação e formação em segurança da informação		
3	Plano anual de workshops de consciencialização	R.7.3	Consciencialização		Art. 24
		R.7.4	Comunicação		Art. 24
		A.7.2.2	Consciencialização, educação e formação em segurança da informação		
		A.9.3.1	Utilização da informação secreta para autenticação		Art. 16, Art. 17
4	Iniciativa anual "Cidadão Ciberseguro" do CNCS	R.7.2	Competência		Art. 24
		A.6.1.3	Contacto com autoridades competentes		Art. 31, Art. 35, Art. 36
		A.7.2.2	Consciencialização, educação e formação em segurança da informação		
5	Formalizar uma política de transferência de informação	A.13.2.1	Políticas e procedimentos de transferência de informação		Art. 5, Art. 7, Art. 15, Art. 20, Art. 26
		A.13.2.2	Acordos sobre a transferência de informação		Art. 5, Art. 7, Art. 20, Art. 26
		A.13.2.3	Mensagens eletrónicas		Art. 5, Art. 7, Art. 20, Art. 26
		A.13.2.4	Acordos de confidencialidade ou de não divulgação		Art. 5, Art. 7, Art. 20, Art. 26

6.7 Iniciativa nº7 - Gestão do Ciclo de Vida Aplicacional

A maior base da sustentação de operações na Rangel deve-se a sistemas aplicacionais, maioritariamente desenvolvidas internamente. Na organização existem várias abordagens ao desenvolvimento aplicacional que devem ser consideradas na Segurança da Informação:

- Desenvolvimento efetuado com recurso às equipas internas, com engenheiros de software internos;
- Desenvolvimento efetuado por engenheiros de software externos, em regime de outsourcing, mas integrados nas equipas de desenvolvimento internas, logo sob as práticas da organização;
- Implementação de plataformas aplicacionais adquiridas a fabricantes externos, porém com customizações por vezes efetuadas por elementos internos, outras vezes contratadas a consultores externos do próprio fabricante ou parceiros;
- Contratação do desenvolvimento *end-to-end* a parceiros externos, podendo a sua manutenção ser assegurada pelo parceiro ou por elementos internos;

Em qualquer uma das formas de desenvolvimento acima mencionadas, cabe à Rangel a gestão dos requisitos e o controlo de qualidade da aplicação.

Tabela 11 - Ações da Iniciativa nº7 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	Processo ITIL	RGPD
1	Políticas e procedimentos para desenvolvimento de software	A.14.2.1	Política de desenvolvimento seguro		
		A.14.2.4	Restrições sobre alterações em pacotes de software		
		A.14.2.5	Princípios de engenharia de sistemas seguros		
		A.14.2.6	Ambiente de desenvolvimento seguro		
2	Políticas e procedimentos para compra e integração	A.14.2.1	Política de desenvolvimento seguro		
		A.14.2.4	Restrições sobre alterações em pacotes de software		

	de *software* comercial	A.14.2.5	Princípios de engenharia de sistemas seguros		
		A.14.2.6	Ambiente de desenvolvimento seguro		
3	Políticas e procedimentos de *outsorcing*	A.14.2.1	Política de desenvolvimento seguro		
		A.14.2.4	Restrições sobre alterações em pacotes de software		
		A.14.2.5	Princípios de engenharia de sistemas seguros		
		A.14.2.6	Ambiente de desenvolvimento seguro		
		A.14.2.7	Desenvolvimento subcontratado		
4	Desenho e implementação de uma metodologia de gestão de mudança	A.12.1.2	Gestão de alterações	Gestão de mudança	
		A.12.5	Controlo de *software* em sistemas de produção		
		A.14.2.2	Procedimentos de controlo de alterações aos sistemas		
5	Desenho e implementação de uma metodologia de validação formal de sistemas	A.14.2.3	Revisão técnica de aplicações após alterações na plataforma de produção	Validação de serviços e testes	
		A.14.2.8	Testes de segurança de sistemas		
		A.14.2.9	Testes de aceitação de sistemas		
		A.14.3	Dados de teste		
6	Desenho e implementação de uma metodologia de requisitos	A.14.1.1	Especificação e análise de requisitos de segurança da informação	Coordenação de design Gestão de catálogo Gestão de capacidade	Art. 5, Art. 6, Art. 7, Art. 9, Art. 10, Art. 11, Art. 12, Art. 13, Art. 14, Art. 15, Art. 16, Art. 17, Art. 18, Art. 19, Art. 20, Art. 21, Art. 22
		A.14.1.2	Proteger serviços aplicacionais nas redes públicas		Art. 14, Art. 16
		A.14.1.3	Proteger transações de serviços aplicacionais		Art. 14, Art. 16

6.8 Iniciativa nº 8 – Gestão de Incidentes (interface com gestão de eventos e problemas)

Segundo os processos do ITIL, a gestão de eventos é considerada uma boa prática e sinal de maturidade em termos de controlo, por isso, deve ser implementada. A Rangel já aplica no seu quotidiano práticas inseridas na gestão de evento. Assim, a iniciativa aqui representada, decorre na interface com gestão de incidentes. Esta iniciativa inclui a monitorização, investigação, intensificação e resposta a eventos que ocorrem ao nível das TI e provocaram uma redução de qualidade desses serviços (definição de incidente), tendo como objetivo filtrar e categorizar esses eventos, de modo decidir as ações apropriadas a tomar. Assim, de forma geral, a iniciativa irá compor-se por:

- Identificar os ativos (de qualquer natureza técnica/tecnológica) relevantes para continuidade do negócio e quais os eventos a monitorizar;
- Manter um inventário de todos os ativos (ex. equipamentos que suportam bases de dados críticas), associados às atividades de processamento de dados pessoais, numa perspetiva de "relações de dependência", para a elaboração posterior de um "data mapping" que permita uma atuação mais automatizada e intervenção rápida no caso de falhas ou potenciais quebras de segurança de dados;
- Definir procedimentos para a Gestão de Incidentes e avaliar a criação de um *Security Operation Center*;
- Aderir e participar na rede de CSIRT, como fórum de partilha de informação de carácter operacional que permita melhorar a capacidade nacional de resposta a incidentes.
- Estabelecer uma classificação de eventos de acordo com o risco/ameaça;
- Criar mecanismos de registo, tratamento e *follow-up* do event;

Adicionalmente, através da das boas práticas de gestão de eventos inserida no plano de resposta a incidentes, a Rangel será capaz de prevenir incidentes que já aconteceram de acontecer outra vez e, se são inevitáveis, ser capaz de reduzir o impacto na atividade de negócio.

- Implementar uma abordagem de uma análise causa-raiz, aumento a eficácia da segurança da informação.
- Através do conhecimento obtido de problemas conhecidos, criação de procedimentos de ação e leitura de forma a minimizar o impacto desses incidentes no negócio.

Um plano de resposta a incidentes bem estruturo e implementado consegue responder e cobrir todos os objetivos desta iniciativa.

Tabela 12 - Ações da Iniciativa nº8 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	Processo ITIL	RGPD
1	Desenhar metodologia de gestão de incidentes	A.16.1.1	Responsabilidades e procedimentos	Gestão de eventos e problemas	Art. 12, Art. 13, Art. 14, Art. 17, Art. 18, Art. 19, Art. 21, Art. 22, Art. 26, Art. 33, Art. 34, Art. 48
2	Implementar plataforma SIEM	A.16.1.2	Reportar eventos de segurança da informação	Gestão de incidentes (interface com gestão de eventos)	Art. 12, Art. 13, Art. 14, Art. 17, Art. 18, Art. 19, Art. 21, Art. 22, Art. 26, Art. 33, Art. 34, Art. 48
3	Definir os eventos a monitorizar	A.16.1.4	Avaliação e decisão sobre eventos de segurança da informação		Art. 12, Art. 13, Art. 14, Art. 17, Art. 18, Art. 19, Art. 21, Art. 22, Art. 26, Art. 33, Art. 34, Art. 48
4	Elaboração do plano de resposta a incidentes	A.16.1.5	Resposta a incidentes de segurança da informação	Gestão de incidentes (interface com gestão de problemas)	Art. 12, Art. 13, Art. 14, Art. 17, Art. 18, Art. 19, Art. 21, Art. 22, Art. 26, Art. 33, Art. 34, Art. 48
		A.16.1.6	Aprender com os incidentes de segurança da informação		Art. 12, Art. 13, Art. 14, Art. 17, Art. 18, Art. 19, Art. 21, Art. 22, Art. 26, Art. 33, Art. 34, Art. 48
		A.16.1.7	Recolha de evidências		Art. 12, Art. 13, Art. 14, Art. 17, Art. 18, Art. 19, Art. 21, Art. 22, Art. 26, Art. 33, Art. 34, Art. 48

6.9 Iniciativa nº9 - Gestão de Atualizações

Esta medida tem o objetivo de corrigir e proteger os sistemas de informação de vulnerabilidades no software e aplicações que são suscetíveis de ataques maliciosos, ajudando, assim, a organização a reduzir o risco de segurança. Esta medida é suportada por uma metodologia de gestão e aplicação controlada de atualizações nas várias camadas da arquitetura tecnológica. Por isso, é necessário manter os ativos tecnológicos atualizados, uma vez que são a principal forma de proteção contar explorações.

No entanto, a Rangel já possui uma política de atualizações ao nível de *endpoints*, no que diz respeito a computadores, contudo, é fundamental estender esta política aos restantes ativos da organização.

Tabela 13 - Ações da Iniciativa nº9 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	Processo ITIL	RGPD
1	Inventariar de ativos	A.8.1.1	Inventário de ativos	*Asset and configuration Management*	Art. 5, Art. 15
2	Gestão dos contratos de manutenção dos ativos				
3	Procedimentos operacionais da gestão de *patchs*	A.12.6.1	Gestão de Vulnerabilidades técnicas		

6.10 Iniciativa nº10 - Segurança Avançada de Perímetro

Esta iniciativa está mais inserida no âmbito na estrutura da estratégia de cibersegurança, no sentido que é linha da frente de defesa contra as ameaças externas e tentativas de intrusão a partir do exterior, exfiltração de dados, *DDoS* (negação de serviços através do consume total dos recursos disponíveis), ataques de vírus informáticos/ *malwares*, entre outros.

Obviamente que esta forma estruturante da estratégia de cibersegurança por si só não assegura o total nível de segurança pretendido com o SGSI. Contudo agrupado com outras iniciativas, é um dos passos mais críticos.

Porém, envolve investimentos com alguma dimensão ao nível de CAPEX e OPEX, nomeadamente na aquisição e suporte anual da next-gen firewall e na ferramenta de proteção dos endpoints.

Atualmente, a Rangel possui já na sua infraestrutura e know-how interno em tecnologia Checkpoint pelo que fará sentido considerar esse vendor. Uma solução como a Checkpoint tem a vantagem de além de ser uma firewall avançada com mecanismos de IPS/IDS, possuir soluções para endpoints PCs/aparelhos móveis (*Sandblast Agent* e *Sandblast mobile*) e também para soluções *cloud*, nomeadamente Office365 usado pela organização, o *Cloudguard SaaS*.

Tabela 14 - Ações da Iniciativa nº10 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	RGPD
1	Implementação de Next-Gen firewalls	A.12.2.1	Proteção contra código malicioso	
2	Segmentação da rede	A.13.1.3	Segregação das redes	Art. 20
3	Política de utilização responsável dos ativos	A.8.1.3	Utilização aceitável de ativos	
		A.12.6.2	Restrições sobre a instalação de software	

	tecnológicos (ex.: equipamentos, software, ...)			
4	Encriptação de *end-points* e *media storage*	A.10	Criptografia	Art. 5
5	Proteção local de *endpoints* (next-gen AV: móvel, pc)	A.12.2.1	Proteção contra código malicioso	
		A.12.6.2	Restrições sobre a instalação de *software*	
6	Definir política e procedimentos de controlo para a contratação de soluções *cloud*	A.13.1.2	Segurança de serviços de rede	Ar. 20
		A.15.1	Segurança da informação nas relações com os fornecedores	Art. 5, Art. 26, Art 27, Art. 28
		A.15.2	Gestão da entrega de serviços pelos fornecedores	Art. 5, Art. 26, Art 27, Art. 28

6.11 Iniciativa nº11 - Gestão de Identidades e Acessos

Esta medida irá criar um modelo que limita o controlo de identidades na organização, respetivos acessos e privilégios a aplicações e dados. Esta iniciativa é constituída por duas vertentes:

- Uma vez que a Rangel já possui medidas técnicas de controlo de acesso às rede e serviços, apenas haverá um reforço através da e construção de uma política documentada de controlo de acessos.

Tabela 15 - Ações da Iniciativa nº11 e seu mapeamento

Nº Ação	Ação	ISO 27001	Controlo	Processo ITIL	RGPD
1	Definir a política de controlo de acessos	A.9.1.1	Política de controlo de acesso	Gestão de Acessos	Art. 5, Art. 16, Art. 17
		A.9.4.1	Restrição de acessos à informação		Art. 5, Art. 16, Art. 17

6.12 Mapeamento dos Objetivos Organizacionais, Oportunidades de Melhoria e Iniciativas

O objetivo desta secção é demonstrar o mapeamento das oportunidades de melhoria, com os respetivos objetivos organizacionais e com as iniciativas. Isto é, sabendo classificação de cada subdimensão das cinco dimensões do estado de maturidade futuro TO-BE, foi correspondido um determinado objetivo de organizacional. Além disso, para cada uma dessas correspondências, não só foi atribuído uma oportunidade de melhoria, uma falha que no estado atual AS-IS para a mesma subdimensão e respetiva

dimensão, mas também foi atribuído a respetiva iniciativa, um conjunto de ações de modo com o objetivo de alcançar o estado futuro ao qual está mapeado.

Tabela 16 - Mapeamento dos objetivos organizacionais, oportunidades de melhoria e iniciativas

Dimensão	Subdimensão	Estágio To-Be	Objetivo Organizacional	Cód. OM	Oportunidade de Melhoria	Cód. In	iniciativa
Visão	Objetivos de Negócio	(4) *Managed*	*Business Continuity Plan*	OM.01	Não existe uma abordagem á gestão pelo risco no desenho das soluções de TI para suportar as iniciativas de negócio	In.01	Promover a Segurança de Informação na Organização
						In.02	Modelo de Governança
						In.03	Reavaliar a Metodologia de Gestão de Projetos
	Objetivos de Segurança	(4) *Managed*	*Business Continuity Plan*				
	Fiscalização Regulatória	(4) *Managed*	Legal / Regulatório	OM.02	Não existem práticas de auditorias internas por forma a antecipar problemas de conformidade	In.04	Implementar Práticas de Auditorias Internas
	Finança/ Economia	(4) *Managed*	Performance Operacional e Financeira	OM.03	Não existe a prática da qualificação dos projetos de investimento	In.03	Reavaliar a Metodologia de Gestão de Projetos
Gestão do Risco	Abordagem do Risco	(4) *Managed*	Performance Operacional e Financeira	OM.03	Não existe a prática da qualificação dos projetos de investimento	In.03	Reavaliar a Metodologia de Gestão de Projetos
	Metodologias/ Medidas	(4) *Managed*	*Business Continuity Plan*				
			Performance Operacional e Financeira				
	Relações Externas	(3) *Repeatable*	*Business Continuity Plan*	OM.04	Não há avaliação à segurança de informação dos parceiros externos	In.05	Relação com Terceiros
			Legal / Regulatório	OM.05	Não existe consideração pelos requisitos de segurança de informação aquando da realização de contratos com os parceiros externos	In.05	Relação com Terceiros
	Ambiente de Controlo	4) *Managed*	*Business Continuity Plan*	OM.01	Não existe uma abordagem á gestão pelo risco no desenho das soluções de TI para	In.10	Segurança Avançada de Perímetro

					suportar as iniciativas de negócio		
Pessoas	Liderança Executiva	(4) *Managed*	*Business Continuity Plan* Legal / Regulatório	OM.01	Não existe uma abordagem á gestão pelo risco no desenho das soluções de TI para suportar as iniciativas de negócio	In.03	Reavaliar a Metodologia de Gestão de Projetos
	Cultura Organizacional	(3) *Repeatable*	*Business Continuity Plan* Legal / Regulatório	OM.06	Não existe uma cultura de participação ativa nos temas de segurança de informação	In.06	Programa de Consciencializaçã o para a Segurança da Informação
	Executivos de segurança (CISO)	(4) *Managed*	*Business Continuity Plan* Legal / Regulatório	OM.06	Não existe uma cultura de participação ativa nos temas de segurança de informação	In.01	Promover a Segurança de Informação na Organização
	Contratação de terceiros para segurança	(3) *Repeatable*					
Processos	Gestão da Confiança	(4) *Managed*	Legal / Regulatório	OM.02	Não existem práticas de auditorias internas por forma a antecipar problemas de conformidade	In.04	Implementar Práticas de Auditorias Internas
	Gestão da Identidade	(5) *Optimized*	*Business Continuity Plan* Legal / Regulatório	OM.07	Não existe um processo de gestão de identidades e acessos aprimorados na organização	In.11	Gestão de Identidades e Acessos
	Gestão de Vulnerabilidades	(4) *Managed*	*Business Continuity Plan*	OM.08	Não existe uma política gestão de atualizações alargada a todos os níveis da arquitetura das redes dos sistemas de informação	In.09	Gestão de Atualizações
				OM.09	Não existe uma prática de segurança *by design* no processo de desenvolvimento de software	In.07	Gestão do Ciclo de Vida Aplicacional
	Gestão de Ameaças	(3) *Repeatable*	*Business Continuity Plan*	OM:10	Não existem práticas de gestão de problemas (*problem management*)	In.08	Gestão de Incidentes
Tecnologias de Segurança	Gestão de Identidade	(2) *Opportunistic*	Legal / Regulatório	OM.11	Não existe monitorização das atividades de utilizadores privilegiados	In.11	Gestão de Identidades e Acessos
	Gestão de Vulnerabilidades	(4) *Managed*	*Business Continuity Plan*	OM.12	Não existe uma solução avançada de segurança ao nível das redes, aplicações e *endpoints*	In.10	Segurança Avançada de Perímetro

	Gestão de Ameaças	(4) *Managed*	*Business Continuity Plan*	OM.12	Não existe uma solução avançada de segurança ao nível das redes, aplicações e endpoints	In.10	Segurança Avançada de Perímetro
	Gestão de Confiança	(2) *Opportunistic*	*Business Continuity Plan*	OM.12	Não existe uma solução avançada de segurança ao nível das redes, aplicações e endpoints	In.10	Segurança Avançada de Perímetro

7. ROADMAPS E REQUISITOS DE CONTROLO

Neste capítulo, será apresentado as duas propostas de soluções, o *Roadmap* da implementação das iniciativas e outra proposta de um Roadmap, de modo a obter uma possível certificação ISO/IEC 27001:2013. Estas propostas representam os *deliveries* deste projeto.

7.1 Roadmap da Implementação das Iniciativas

Em primeiro lugar, será apresentado uma proposta de *Roadmap* de implementação das iniciativas apresentadas no capítulo anterior, que cobrem vários requisitos e controlos da norma internacional.

7.1.1 Identificação dos controlos ISO 27001:2013 Implementados

No capítulo 6, são apresentadas as diferentes iniciativas, de modo a alcançar um estado de maturidade futuro, To-Be, a partir do estado de maturidade atual, As-Is. De seguida, no capítulo anterior, também é realizado um mapeamento de cada ação de cada uma das iniciativas, com os requisitos e controlos da ISO 27001:2013 a que relacionam, juntamento com os artigos a que correspondem no RGPD. Assim, nesta secção, foi igualmente identificado os controlos já implementados pelo Grupo Rangel, que se apresentam enumerados na seguinte tabela:

Tabela 17 - Lista de controlos já implementados

Cód. ISO	Designação ISO	Artigo RGPD
A.6.1.1	Papéis e responsabilidades de segurança da informação	
A.6.1.2	Segregação de funções	
A.6.2.1	Política de dispositivos móveis	
A.6.2.2	Teletrabalho	
A.9.1.2	Acesso a redes e a serviços de rede	Art. 16, Art.17
A.9.2.1	Registo e cancelamento de utilizador	Art. 16, Art.17
A.9.2.2	Disponibilização de acesso aos utilizadores	Art. 16, Art.17
A.9.2.3	Gestão de direitos de acesso privilegiado	Art. 16, Art.17
A.9.2.4	Gestão da informação secreta para autenticação de utilizadores	Art. 16, Art.17
A.9.2.5	Revisão de direito de acesso de utilizadores	Art. 16, Art.17
A.9.2.6	Remoção ou ajuste de direitos de acesso	Art. 16, Art.17
A.9.4.2	Procedimentos seguros de início de sessão	Art. 16, Art.17
A.9.4.3	Sistema de gestão de senhas	Art. 16, Art.17
A.9.4.5	Controlo de acesso ao código fonte de programas	Art. 16, Art.17
A.11.1.1	Perímetro de segurança física	
A.11.1.2	Controlos de entrada física	

A.11.1.3	Segurança em escritórios, salas e instalações	
A.11.1.4	Proteção contra ameaças externas e ambientais	
A.11.2.2	Serviços básicos de suporte	
A.11.2.3	Segurança de cablagem	
A.11.2.4	Manutenção de equipamentos	
A.11.2.6	Segurança de equipamentos e ativos fora das instalações	
A.11.2.7	Eliminação e reutilização seguras de equipamentos	
A.11.2.9	Política de secretária limpa e ecrã limpo	
A.12.1.1	Procedimentos de operação documentados	Art. 7, Art. 12, Art.13, Art. 14, Art. 15, Art. 16, Art. 18, Art. 19, Art. 21, Art. 22
A.12.1.4	Separação entre ambientes de desenvolvimento, teste e de produção	
A.12.4.1	Registo de eventos	
A.12.4.2	Proteção da informação registada	
A.12.4.3	Registos de administrador e de operador	
A.12.4.4	Sincronização de relógio	
A.13.1.1	Controlos de rede	Art. 20
A.16.1.3	Reportar pontos fracos de segurança da informação	Art. 12, Art.13, Art. 14, Art. 17, Art. 18, Art. 19, Art. 21, Art. 22, Art. 26, Art. 33, Art. 34, Art. 48
A.17.1.1	Planeamento da continuidade de segurança da informação	Art. 5
A.17.1.2	Verificar, rever e avaliar a continuidade de segurança da informação	Art. 5
A.17.1.3	Implementação da continuidade de segurança da informação	Art. 5
A.17.2.1	Disponibilidade dos recursos de processamento da informação	Art. 5

7.1.2 Identificação dos controlos ISO 27001:2013 não cobertos

Concluindo a análise dos controlos já implementados pela organização, foi realizado, de igual forma, uma identificação dos controlos da norma internacional, além dos artigos do RGPD, que não têm correspondência, ou seja, não são cobertos pelas iniciativas que serão implementadas, de modo a atingir o estado de maturidade To-Be, nem os que eram cobertos pelo estado As-Is. Deste modo, não só foi determinado os controlos da norma em falta (tabela 5), como também, no final, foi identificado os controlos não aplicáveis (tabela 6).

Tabela 18 - Lista de controlos em falta

Cód. ISO	Designação ISO	Artigo RGPD
A.7.2.3	Procedimento disciplinar	
A.7.3.1	Responsabilidades na cessação ou alteração da relação contratual	
A.8.1.2	Responsabilidade pelos ativos	
A.8.1.4	Devolução de ativos	
A.8.2.1	Classificação da informação	Art. 5, Art. 9, Art. 10, Art. 11, Art. 13, Art. 15, Art. 18, Art. 35, Art. 36
A.8.2.2	Etiquetagem da informação	Art. 5
A.8.2.3	Manuseamento de ativos	Art. 5, Art.7, Art. 9, Art.10, Art. 11, Art. 13, Art. 14, Art. 18
A.8.3.1	Gestão de suportes de dados amovíveis	Art. 5, Art. 20
A.8.3.2	Eliminação de suportes de dados	Art. 5, Art. 7, Art. 17, Art. 20
A.8.3.3	Transporte de suportes de dados	Art. 5, Art. 20
A.11.1.5	Trabalhar em áreas seguras	
A.11.1.6	Áreas de carga e descarga	
A.11.2.1	Colocação e proteção de equipamentos	
A.11.2.5	Remoção de ativos	
A.11.2.8	Equipamento de utilizador não vigiado	
A.12.1.3	Gestão da capacidade	
A.12.3.1	Salvaguarda de informação	Art. 16, Art. 17, Art. 18, Art. 21
A.18.1.1	Identificação da legislação aplicável e de requisitos contratuais	Art. 5, Art. 6, Art. 18, Art. 23, Art. 26, Art. 28, Art. 85, Art. 86, Art. 87, Art. 88, Art. 90, Art. 92, Art. 93, Art. 94, Art. 95, Art. 96, Art. 97, Art. 98, Art. 99
A.18.1.2	Direitos de propriedade intelectual	Art. 5, Art 26
A.18.1.3	Proteção de registos	Art. 5, Art. 7, Art. 16, Art. 20, Art. 26, Art. 28
A.18.1.4	Privacidade e proteção de dados	Art. 1, Art. 3, Art. 5 Art. 26, Art. 27, Art. 28, Art. 33, Art. 34, Art. 37, Art. 38, Art. 39, Art. 40, Art. 41, Art. 42, Art. 43, Art. 45, Art. 46, Art. 47, Art. 48, Art. 49, Art. 82, Art. 83, Art. 84, Art. 85, Art.

		86, Art. 87, Art. 88, Art. 89, Art. 90, Art. 91
A.18.1.5	Regulamentação de controlos criptográficos	Art. 5, Art. 26
A.18.2.1	Revisão independente de segurança da informação	Art. 5
A.18.2.2	Conformidade com as políticas e normas de segurança	Art. 5
A.18.2.3	Revisão da conformidade técnica	Art. 5

Tabela 19 – Lista de controlos não aplicáveis

Cód. ISO	Designação ISO	Artigo RGPD
A.9.4.4	Utilização de programas utilitários privilegiados	Art. 16, Art. 17

Depois do mapeamento das iniciativas com a norma ISO/IEC 27001:2013, chegou-se à conclusão de que estas cobrem um total de 52 dos 114 controlos, abrangendo 23 dos 35 objetivos de controlo. Sabendo que, um dos controlos não cobertos pelas iniciativas não se aplica ao Grupo Rangel e 36 destes controlos já se encontram implementados pela organização, conclui-se também que, de modo a obter uma possível certificação da norma, existe um défice de 25 controlos que tem de ser suprimido.

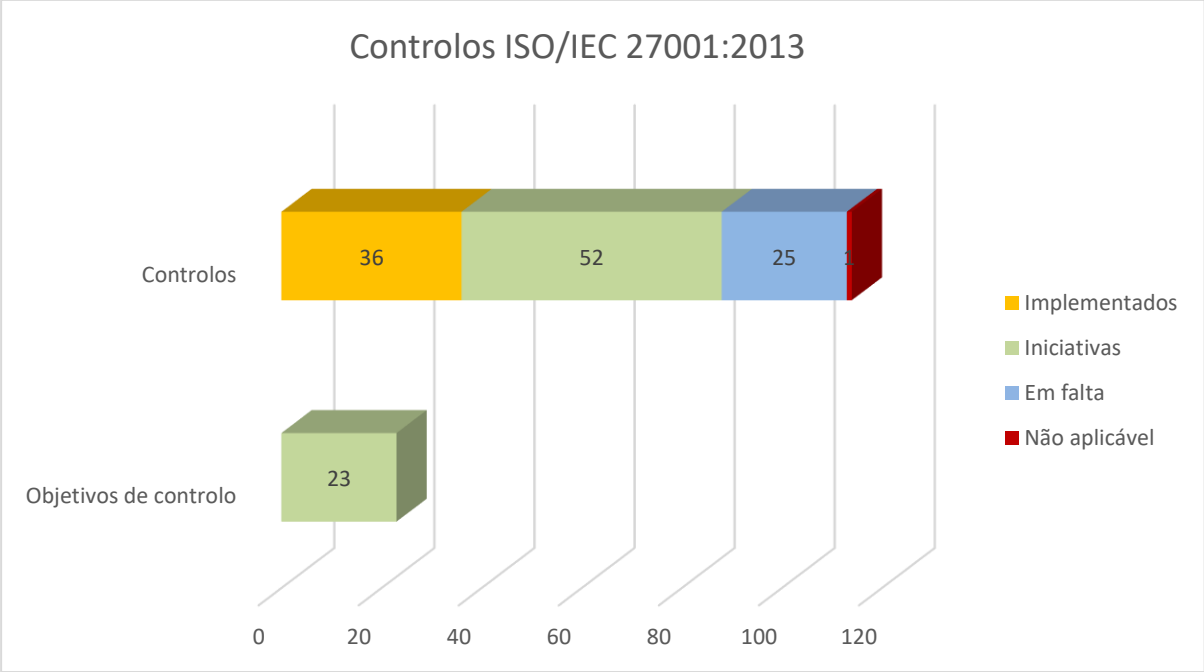


Figura 29 - Controlos e requisitos da norma ISO/IEC 27001:2013

7.1.3 Calendarização do Roadmap

Nesta secção será apresentado uma sugestão do *Roadmap*. A distribuição da implementação das várias iniciativas será apresentada no diagrama abaixo representado (*Figura 30*). As iniciativas estão distribuídas

em várias fases, podendo mais do que uma iniciativa decorrer em simultâneo, devido as características e elementos comuns, e por motivos de agilização do projeto.

Como referido no capítulo 2, por mais que as organizações invistam em medidas técnicas, como por exemplo, a aquisição de mecanismos de defesa, *firewall*, *softwares* mais atualizados do mercado, entre outras medidas, estas organizações não estão livres de ameaças, uma vez que a maior vulnerabilidade numa organização é fator humano. Assim, pretende-se começar primeiramente com as iniciativas focadas na consciencialização e configuração para uma mentalidade direcionada para a segurança da informação, para além do comportamento humano na organização (gestão da mudança e *sponsorship)*. Só depois destas desta filosofia estiver assente e imposta em prática na organização, é que se foca nas iniciativas mais operacionais e/ou baseadas em controlos técnicos. Esta forma de distribuição pretende promover o sucesso do projeto.

Estima-se que o total da implementação de todas as iniciativas identificadas ocupará um espaço temporal de 13 meses.

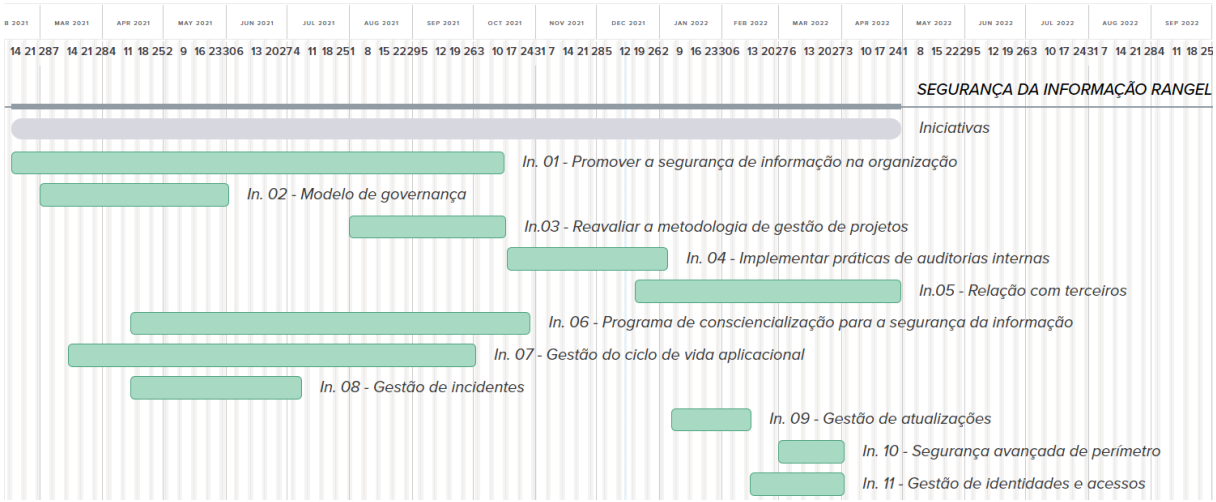


Figura 30 - Roadmap da Iniciativas propostas

Fazendo a atribuição de responsabilidades parte dos requisitos da norma internacional, foi atribuído a cada uma das iniciativas, um ou mais responsáveis pela sua implementação. Na tabela abaixo (Tabela 22) mostra a correspondência das iniciativas com os seus respetivos responsáveis. Os responsáveis associados às iniciativas podem ser:

- Gestão de topo (GT)
- *Chief Information Security Officer* (CISO – cargo criado na para a coberta da norma)
- Comitê para a segurança de Informação (CSI)
- *Deputy* (DEP)

Tabela 20 - Responsáveis por cada iniciativa

Cód. IN	Designação da Iniciativa	Responsável
IN. 01	Promover a segurança de informação na organização	GT, CISO, CSI
IN. 02	Modelo de governança	GT, CISO, CSI
IN. 03	Reavaliar a metodologia de gestão de projetos	CISO, CSI
IN. 04	Implementar práticas de auditorias internas	CISO
IN. 05	Relação com terceiros	GT, CISO, CSI
IN. 06	Programa de consciencialização para a segurança da informação	CISO, DEP
IN. 07	Gestão do ciclo de vida aplicacional	CISO, CSI
IN. 08	Gestão de incidentes	DEP (DSI)
IN. 09	Gestão de atualizações	DEP (DSI)
IN. 10	Segurança avançada de perímetro	DEP (DSI)
IN. 11	Gestão de identidades e acessos	DEP (DSI)

7.2 Roadmap dos Controlos em não cobertos

O estado futuro, TO-BE, não abrange a implementação de controlos suficientes para uma possível obtenção de uma certificação da norma ISO 27001:2013. Portanto, de modo a ter como meta essa possível certificação, o grupo Rangel procedeu um *Gap Analysis*, de modo a identificar quais os controlos que não cobertos nem pelo estado atual, AS-IS, nem pelo conjunto de iniciativas que juntamente com o estado AS-IS originam o estado futuro. A identificação desses controlos é possível observar na tabela 20, no subcapítulo 7.1.2. De seguida, foi criado um programa posterior e específico, sendo sugerido o início deste programa logo após o término do programa de implementação de iniciativas. É esperado que estes dois programas em conjunto, alcancem uma cobertura total da norma internacional, não sendo um dos controlos da ISO (ver tabela 21) aplicável à atividade de trabalho do grupo Rangel.

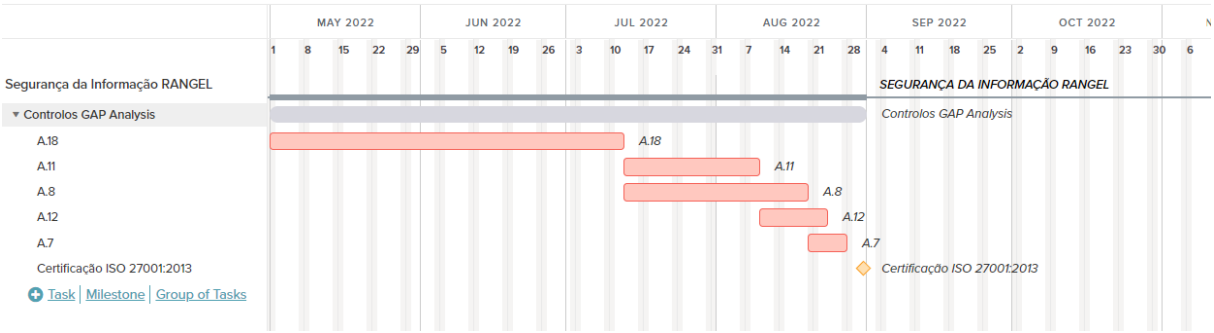


Figura 31 - Roadmap dos controlos não cobertos pelas iniciativas

Como é observável na figura acima, o programa de implementação dos controlos que não foram cobertos pelo programa de iniciativas tem uma duração, aproximadamente, de 4 meses, pelo que, no final desse período será possível obter uma certificação da norma internacional ISO 27001:2013.

Começando pela implementação dos controlos da cláusula de controlo de segurança A.18, uma vez que este apresenta o maior número de controlos em falta (neste caso, todos os objetivos de controlo - 2 - e respetivos controlos – 8) e consequentemente maior representatividade no mapeamento dos artigos do RGPD, sendo mapeados 30 artigos no total.

Seguidamente, iniciou-se a implementação dos controlos das cláusulas de segurança A.11 e A.8 com períodos de implementação diferentes. Esta diferença deve-se também ao diferente número de controlos por implementar em cada um, respetivamente. A cláusula de controlos de segurança A.11 tem um total de 15 controlos de segurança (ver tabela 1) tendo já sido implementado 10 controlos, ficando, deste modo, 5 controlos por realizar. Estes 5 controlos em falta não têm qualquer correspondência com os artigos do regulamento. Relativamente à execução dos controlos em falta da cláusula de controlos de segurança A.8, foi necessário executar 8 controlos, na maneira que esta cláusula apresenta um total de 10 controlos (tabela 1, capítulo 2) e 2 estão planeados para serem implementados no plano de iniciativas; mais concretamente na iniciativa nº9 (A.8.1.1) e iniciativa nº10 (A.8.1.3).

Por fim, as tarefas menos duradouras foram as cláusulas A.7 e A.12, visto que faltavam implementar 2 controlos em ambas. A cláusula de controlos de segurança A.12 tem um total de 14 controlos (tabela 1, capítulo 2) dispersos por 7 objetivos de controlo, pelo que 6 controlos já tinham sido realizados e outros 6 foram englobados no plano de iniciativas (iniciativa nº4 - A.12.7.1; iniciativa nº7 - A.12.1.2 e A.12.5.1; iniciativa nº9 - A.12.6.1; iniciativa nº10 - A.12.2.1 e A.12.6.2). Distintamente, a cláusula A.7 apresenta 6 controlos (tabela1) sendo que destes 6, 4 estão inseridos no plano de iniciativas (iniciativa nº5 - A.7.1.1, A.7.1.2 e A.7.2.1; iniciativa nº6 - A.7.2.2).

7.3 Conformidade com o RGDP

Como referido e explicado num capítulo antecedente deste documento, (capítulo 3), um dos objetivos da sua estratégia é o objetivo organizacional Legal/Regulatório, sendo por si só, já um objetivo de extrema relevância.

Contrariamente ao que foi realizado para norma internacional ISO/IEC 27001:2013, não é necessário fazer uma análise quantidade do grau de cobertura do RGPD no sentido de alcançar qualquer tipo de certificação ou cumprimento integral. Uma vez que não existe nenhum tipo de certificação para o regulamento, também não é esperado que as empresas implementam todos os 99 artigos do RGPD. Na

prática, na medida de evitar o uso desnecessário de recursos de uma organização, as empresas apenas cumprem o mínimo de conformidade para evitar investigações, coimas e penalizações que provocam impactos negativos à organização.

Um dos pontos de ação crucial de forma a cumprir o regulamento é a realização de "avaliações de impacto", mais conhecidos por DPIAs, na língua oficial inglesa (*Data Privacy Impact Assessment*), que devem sempre ser realizados aquando de uma alteração organizacional relevante, em atividades de processamento, de modo a identificar os riscos de violação de dados pessoais que possam ocorrer. Assim, é pretendida a documentação, por parte da entidade controladora, descrevendo os processos de tratamento de dados pessoais que podem estar em risco, tal como, medidas de salvaguarda e controlos necessários para a mitigação desses riscos. Estas atividades realizam-se, por exemplo, na recolha de dados sensíveis dos colaboradores como a "implementação" de termómetros infravermelhos acoplados a sistemas de vídeo vigilância nas entradas das instalações da Rangel, após o início da epidemia mundial atual que aconteceu antes da realização deste projeto. Um outro exemplo, aconteceu na parceria da Rangel com a Superbock, empresa de produção de cerveja nacional, onde foi exigido por este parceiro, aquando da receção dos camionistas de mercadorias da Rangel, a obrigação de registo por impressão digital. Por motivos evidentes, esta atividade apresenta elevado risco de violação de direitos das pessoas, neste caso, dos colaboradores, o que provoca a realização de uma avaliação de impacto.

Com esta seção, é pretendido destacar o contributo que o Roadmap das Iniciativas, juntamente com uma certificação posterior do SGSI, pode oferecer à organização em termos de conformidade com o regulamento europeu. Esta resposta será medida pela análise quantitativa dos artigos mapeados nos controlos já implementados pela Rangel e os que serão implementados e inseridos nas iniciativas.

Na tabela 19, na secção 7.1.1, com a análise e avaliação do estado da maturidade atual, é possível visualizar os controlos da ISO 27001 já implementados pelo Grupo Rangel e respetivo mapeamento dos artigos do regulamento.

Tabela 21 - Mapeamento de controlos ISO e artigos RGPD (Estado Atual)

N° de Requisitos + Controlos ISO 27001:2013	**36**
N° de Artigos do RGPD rastreados	**16**

Através das iniciativas demonstradas na secção 6, pode-se mapear os controlos implementados nas respetivas ações e artigos RGPD correspondestes, representado na tabela abaixo:

Tabela 22 - Mapeamento de controlos ISO e Artigos RGPD (Iniciativas)

N° de Requisitos + Controlos novos ISO 27001:2013	**26** Requisitos + **52** Controlos

N° de Artigos novos do RGPD rastreados	**22**

Após a implementação das iniciativas e realização das respetivas ações, é de salientar o mapeamento de um total de 38 artigos, sendo que só na lista de iniciativas estão presentes o **total dos 38**, dos quais **22 são artigos novos mapeados**, para além dos **16 mapeados a análise ao estado atual**, representando, assim, o nível de cobertura do estado futuro, $16 + 22 = 38$.

Depois da implementação de todos os conjuntos de ações, que fazem parte das iniciativas, depara-se com um défice de 25 controlos que são necessários para a possível obtenção da certificação da norma internacional ISO 27001:2013. Como é possível observar na tabela 20, no secção 7.1.2, esses controlos contribuem com o mapeamento de 54 artigos do RGPD no total, dos quais **24 são novos** artigos do RGPD não mapeados anteriormente, nem no estado atual nem no plano de iniciativas. Assim, atinge-se um total de 62 artigos mapeados do RGPD, $38 + 24 = 62$.

Na realização deste mapeamento é quase obrigatório destacar os controlos A.18.1.1 e A.18.1.4, uma vez que são os controlos que respondem a mais artigos novos do RGPD, contribuindo assim para o aumento da resposta, sendo o último controlo com foco específico à privacidade e proteção de dados pessoais.

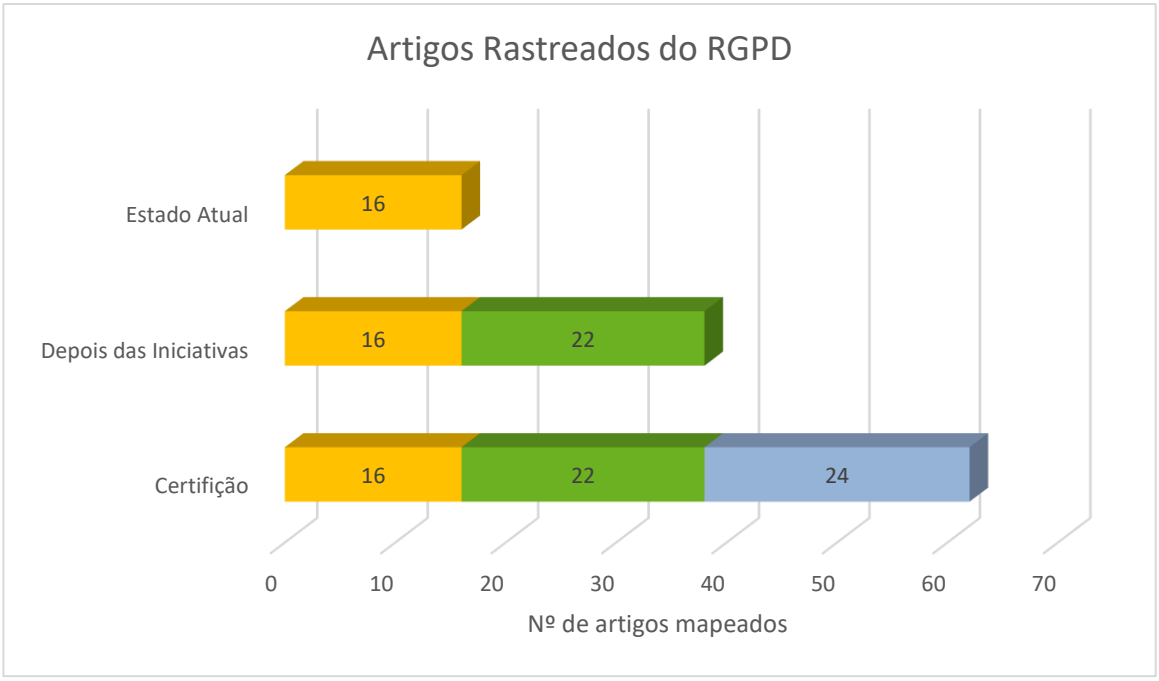


Figura 32 - Etapas da resposta ao RGPD

O gráfico ilustrado acima, através do mapeamento dos artigos com os respetivos controlos da ISO27001:2013 que foram implementados ao longo da estratégia, representa a evolução da resposta ao RGPD e o aumento da maturidade da segurança de informação da Rangel, permitindo assim, concluir

que a adoção dos controlos da norma contribui de forma sustentada, rigorosa e assertiva uma resposta ao RGPD.

Apesar de uma certificação da norma internacional ou adoção parcial dos controlos da mesma, não assegurar automaticamente o cumprimento dos requisitos da norma, as organizações que apresentam a certificação da norma estão "a meio caminho" da conformidade com o RGPD. Portanto, organizações que já apresentam uma estrutura de referência ISO 27001:2013, não sofrerão a duplicação de esforço ou retrabalho, custos adicionais e tempo de forma a cumprir os requisitos do regulamento.

Por outro lado, existem requisitos específicos do regulamento não cobertos pelos controlos da norma associados com a privacidade de dados relacionado com os direitos do titular dos dados, sendo eles:

- Consentimento (Capítulo 2, Artigo 7 do RGPD);
- Direito de portabilidade dos dados (Capítulo 3, Secção 3, Artigo 20 do RGPD);
- Cumprimento dos direitos ARCO:
  - Direito de acesso à informação (Capítulo 3, Secção 2, Artigos 15 do RGPD);
  - Direito de retificação (Capítulo 3, Secção 3, Artigos 16 do RGPD);
  - Direito ao apagamento dos dados ("direito de ser esquecido") (Capítulo 3, Secção 3, Artigo 17 do RGPD);
  - Direito de oposição (Capítulo 3, Secção 4, Artigo 21 do RGPD);
- Direito à limitação do tratamento (Capítulo 3, Secção 3, Artigo 18 do RGPD);
- Transferências de dados pessoais para países terceiros ou organizações internacionais (Capítulo 5 do RGPD);

Para além destes direitos do titular dos dados, existem outros requisitos específicos que a Rangel necessita de endereçar:

- Avaliação de impacto das operações de tratamento suscetíveis de implicar um elevado risco para os direitos e liberdades das pessoas singulares (Capítulo 4, Secção 3, Artigo 35 do RGPD);
- Elaboração de um plano de comunicação (ao titular dos dados e autoridades de controlo) de violações de dados pessoais (Capítulo 4, Secção 2, Artigos 33 e 34 do RGPD);
- Nomeação de um DPO;

Este último, foi um requisito prontamente abatido pela Rangel através da nomeação de uma colaborada externa para o cargo - Catarina Azevedo - licenciada em Direito com pós-graduação em segurança da informação.

- Cumprimento dos requisitos de tratamento de categorias especiais de dados pessoais;

- Cumprimento dos princípios relativos ao tratamento de dados pessoais, tais como: licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade e responsabilidade do responsável pelo tratamento;

8. Ações Executadas e Resultados*

Neste capítulo é demonstrado a realização de algumas ações inseridas no plano de ações das iniciativas propostas no capítulo 6, de forma a executar o Roadmap proposto (secção 7.1), pelo que é esperado uma melhoria no nível de maturidade dos sistemas de informação e, consequentemente, uma maior conformidade com o RGPD.

Aqui, será possível observar todas as ações concretizadas ao longo do período de investigação na Rangel.

8.1 Ações realizadas para a Iniciativa nº1

De maneira a cumprir o plano de ações da iniciativa nº1 - Promover a Segurança de Informação na Organização – fiquei responsável na participação da elaboração da política (Apêndice 2). Não só a política para a segurança da informação é uma grande passo para o aumento do nível de maturidade de segurança e muito importante para a execução do Roadmap proposto, mas também, é um documento que pertence ao conjunto de documentos obrigatórios no SGSI para a certificação da norma.

Esta tarefa foi executada pela DPO e pelo investigador, sob a supervisão do Engenheiro-chefe Luís Correia, e estando concluída, esta fica, assim, a cumprir o requisito R.5.2 e o controlo de segurança da norma A.5.1.1.

Adicionalmente a esta ação, uma outra ação complementar surgiu no âmbito aumentar a maturidade de segurança da informação e, consequentemente, de forma a garantir um maior alinhamento com o RGPD.

- Rever Instruções/Politicas para a adoção de boas práticas quanto ao uso de ferramentas corporativas (ex. portátil, correio eletrónico, contactos, etc.), tendo em vista promover o desuso do email para fins pessoais e o registo e armazenamento de contactos e ficheiros localmente. Atualmente, cada colaborador possui os "seus" contactos no Outlook (e os dispositivos móveis estão sincronizados) o que incrementa o risco de perda ou exposição;

De forma a cumprir a realização desta ação, foi elaborado duas instruções de trabalho (Apêndice 3) sobre o uso da ferramenta corporativa *Onedrive*, com o fim de responder à ação proposta em cima, e uma atualização na política de dispositivos móveis.

8.2 Ações realizadas para a Iniciativa nº2

À luz do plano de ações da iniciativa nº2 - Modelo de Governança – foi estabelecido um plano de comunicações que garante o contacto permanente entre todas as partes interessadas, equipa interna os seus congéneres nos subcontratados e a entidade de controlo (CNPD). Posteriormente, este plano é incorporado e relevante no plano de resposta a incidentes, pelo que na identificação de incidentes, caso

exista a violação de dados pessoais (ex. fuga de dados) o mesmo procedimento apresentado no Apêndice 4 deve ser seguido.

- Desenvolver um plano de comunicação que garanta o contato permanente entre a equipa interna, os seus congéneres nos subcontratados e a entidade de controlo (CNPD)

8.3 Ações realizadas para a Iniciativa nº6

De maneira a cumprir o plano de ações da iniciativa nº6 - Programa de Consciencialização para a Segurança da Informação – primeiramente, foi delineado que para cada novo colaborador que fosse admitido na organização, teria que participar, não só numa formação sobre o regulamento geral de proteção de dados, como também numa formação sobre segurança da informação.

A primeira formação é presenteada pela DPO, onde o participante fica a par sobre os conceitos gerais do regulamento, que entrou em vigor a partir de maio de 2018, como os princípios, consentimento, dados pessoais, dados sensíveis, intervenientes, suas obrigações e responsabilidades, e por fim as coimas. Por exemplo, a formação reponde a algumas perguntas como:

- O que é o RGPD?
- Quem deve cumprir o regulamento?
- A diferença entre proteção de dados e Cibersegurança;
- O que são dados pessoais? E exemplos;
- O que são atividades de tratamento?
- Quando é que se pode recolher e tratar dados?
- Quais são os direitos dos titulares?
- Entre outras

A segunda formação também se insere no plano de formação inicial de um novo colaborador presenteada por um elemento da equipa de segurança da informação. Esta formação abrange vários campos da segurança da informação com o objetivo de informar o participante de uma forma geral. Nesta formação são abordados temas como os princípios da segurança da informação, ataques informáticos, suas formas e objetivos, para além de cuidados a ter e exemplos de boas práticas em diversas ocasiões e locais:

- Palavras-passe e o acesso à informação;
- Posto de trabalho ("*Clean desk*");
- Computador Pessoal;
- Documentos;
- Correio eletrónico;

- Navegação na internet;
- Comunicação;
- Dispositivos móveis;
- Interação com parceiros externos (antes do contrato, durante a relação de negócio; terminada a relação de negócio);
- Destruição de dados,
- Acesso remoro e teletrabalho;
- Redução de riscos (comportamento seguro e indícios suspeitos)

Adicionalmente, de modo a cumprir o plano de ações da iniciativa, foi criado um simulacro para testar, em termos operacionais, a boa adoção dos procedimentos e práticas dos colaborados aprendidos nas formações indicadas anteriormente. Este teste desenvolve-se no âmbito de avaliar a capacidade de denúncias e reportar comportamentos e indícios suspeitos nas atividades de correio eletrónico. Visto isto, o simulacro define-se por um envio de um e-mail por uma entidade externa, ou seja, uma tentativa *Phising*, a fazer-se passar por um colaborador da Rangel de um departamento diferente, neste caso dos recursos humanos da organização.

Figura 33 - Simulacro - Envio de email malicioso

Primeiramente, foi realizado um teste inicial a todos os elementos da equipa de segurança de informação. De todos as mensagens eletrónicas enviadas, neste caso, um total de 7, todas as 7 foram reportadas corretamente.

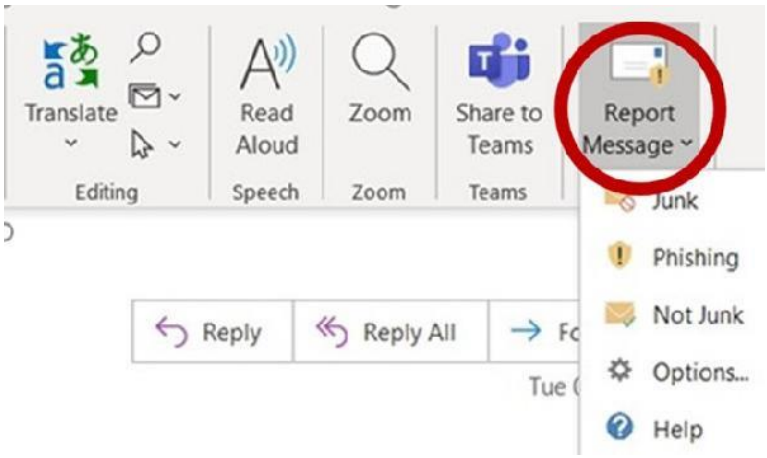


Figura 34 - Procedimento correto de denúncia Phising

Pode-se concluir que todos os elementos da equipa de segurança de informação encontram-se a par das boas práticas de segurança da informação, uma vez que 100% das tentativas de infiltração foram deligadas corretamente. Contrariamente, quando o teste foi, posteriormente, proposto a outros colaborados, um total de 150 colaboradores de várias LoB escolhidos aleatoriamente, apenas 71 colaborados foram capazes de reportar corretamente. Curiosamente, destes 150 colaboradores, 38 colaboradores clicaram no link que supostamente os concedia mais 1 dia de férias que não tinham até ao momento desfrutado, assumindo assim, que os restantes 41 colaboradores ignoram o e-mail, o que por um lado, não é errado, uma vez que assim, não coloca em risco diretamente a segurança da organização, no entanto, não é a melhor prática. Assim, os dados finais deste teste, apontam que 47%dos colaborados denunciaram corretamente sobre esta tentativa de infiltração, 25% dos colaborados não estão familiarizados com a boas praticas de denuncias de atividades suspeitas e outros 27% ignoraram ou decidiram voluntariamente não denunciar nem clicar no link inserido no e-mail malicioso.

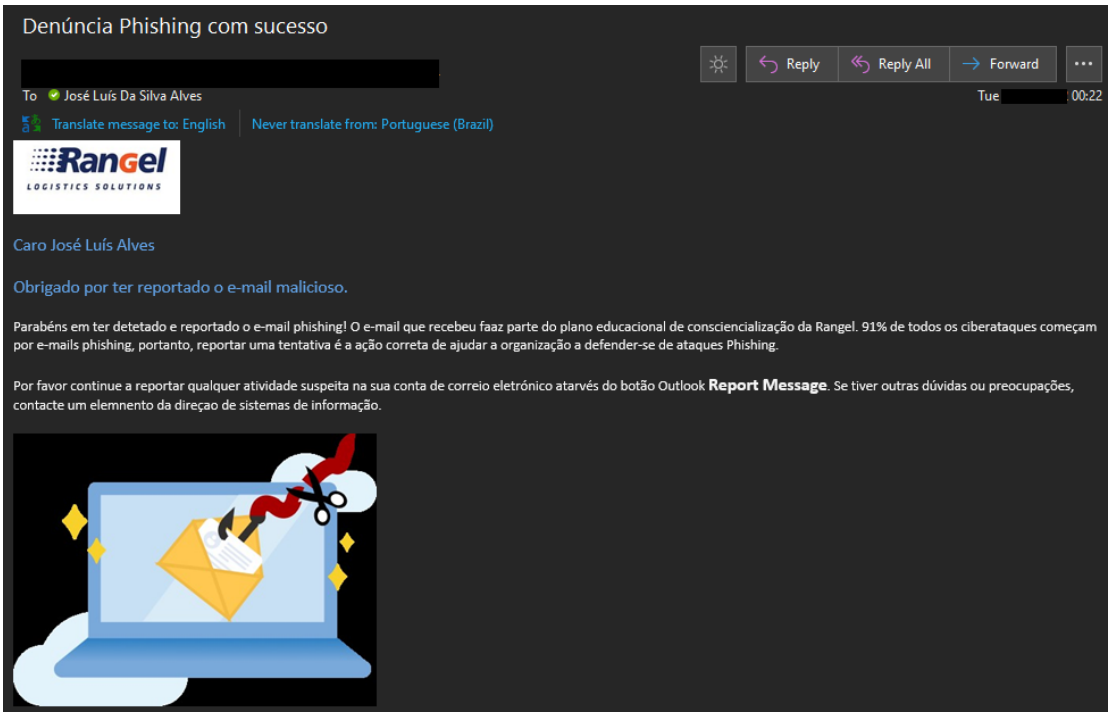


Figura 35 - Resposta automática de denúncias bem-sucedidas

Por fim, no final deste segundo simulacro, foi emitido um comunicado para toda a organização, indicando qual era, numa situação semelhante, a prática mais correta e aconselhando a realizar uma revisão da formação sobre a segurança da informação.

Quer as duas formações da formação inicial quando da entrada de um novo colaborador, quer a realização do simulacro respondem a um controlo de segurança da norma internacional, cobrindo o controlo A.7.2.2.

8.4 Ações realizadas para a Iniciativa nº8

Como indicado no subcapítulo Iniciativa n° 8 – Gestão de Incidentes (interface com gestão de eventos e problemas)6.8, um bom plano de resposta a incidentes, devidamente estruturado e implementado, consegue responder e cobrir todo o plano de ação da iniciativa n°8 - Gestão de Incidentes (interface com gestão de eventos e problemas).

Para tal foi desenvolvido o Plano de resposta a incidentes. Este plano descreve o modo de procedimento das 6 etapas que o constitui (Preparação, Identificação, Contenção, Eliminação, Recuperação, Lições Aprendidas). Nele estão inseridos processos de identificação de incidentes, categorização dos tipos de incidentes por níveis de severidade, identificação da equipa e respetivas responsabilidades, colheita de evidências, entre outros.

Este plano de reposta a incidentes realiza uma cobertura de vários controlos (6) da ISO 27001:2013, dos quais são: A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7.

8.5 Ações Complementares

Na realização de novos *tenders*, concursos públicos pelos quais é realizada a seleção da melhor empresa que apresente a melhor proposta (na prática, a organização capaz de providenciar os bens ou serviços pelo preço mais barato), havia o levantamento de oportunidades de melhoria quando a Rangel não conseguia cumprir um requisito ou possuía uma pobre cobertura do mesmo. Uma das oportunidades de melhoria levantada nestas atividades foi "Não existe documentação que identifique os processos e os sistemas relativos aos planos de continuidade de negócio". Para tal, a Rangel decidiu desenvolver duas instruções de trabalho de forma a responder a esta oportunidade de melhoria e permitir que a Rangel tenha uma posição mais forte nos próximos *tenders*.

A duas Instruções de trabalhos criadas foram:

- *Disaster Recovery* do *Datacenter* – Memória Descritiva e Processo de Teste;
- Gestão de Backups de Dados;

Ambos os documentos (ou partes) podem ser consultados no Apêndice 4 e 5, contudo, alguns elementos aparecem ilegíveis por motivos de confidencialidade.

Assim, a Rangel reforça a sua capacidade de resposta aos controlos da norma cobrindo os controlos A.17.1.1, A.17.1.2 e A.17.1.3.

9. Conclusões e Propostas de Trabalho Futuro

Neste último capítulo, apresentam-se a principais conclusões do trabalho apresentado neste projeto de dissertação, confrontando-se os objetivos do projeto e o que foi desenvolvido para os atingir. Por fim, é realizada uma reflexão acerca das limitações do projeto e, por conseguinte, é sugerido algumas propostas de trabalho futuro, de modo a alcançar a certificação da norma internacional ISO 27001:2013 e alcançar um nível de maturidade alinhado com as obrigações do RGPD.

9.1 Considerações Finais

A presente dissertação teve como objetivo principal a melhoria dos níveis de maturidade para a segurança das tecnologias de informação da *Rangel Logistics Solutions*. Para a concretização do objetivo, pretendia-se a implementação das boas práticas ao nível da segurança da informação, pelo que, a implementação das práticas da norma internacional ISO 27001:2013 de modo a adotar um modelo adequado para estabelecer, implementar, operar, monitorizar, rever e gerir um sistema de gestão de sistemas de informação.

Deste modo, previamente ao desenvolvimento de soluções, foi efetuada uma análise ao estado atual ao nível de segurança dos sistemas de informação da Rangel, pelo que, foi possível perceber e diagnosticar potenciais problemas e oportunidades de melhoria (Tabela 5). Através da *framework MaturityScpape – IT Security 2* do IDC foi possível realizar essa análise, e consequentemente, destacam-se, assim, nas cinco dimensões (visão, gestão de risco, pessoas, processos e tecnologias de segurança), um nível de maturidade de segurança das TI muito baixo. Este nível baixo resulta também de um nível baixo de maturidade das cinco dimensões e respetivas subdimensões, tendo-se constatado que, a dimensão "visão" apresenta um nível de 2,75, um nível de 2,25 para as dimensões "gestão de risco" e "pessoas", e as dimensões "processos" e "tecnologias de segurança" registam o nível mais baixo, cerca de 2. Deste modo, determinou-se que, o nível de maturidade de segurança das TI culmina também num nível baixo, cerca de 2,25.

Tendo em conta os o alinhamento estratégico dos objetivos da rangel para a segurança de informação, na fase de diagnóstico foi possível reportar falhas ou situações que podem justificar uma ação. Visto isto, foram levantas várias oportunidades de melhoria que serviram de base para estabelecer novos níveis de maturidade para a segurança da TI, obtendo assim um novo estado futuro para a organização. Este novo estado tem um nível de maturidade de segurança de 3,65, resultando num aumento de maturidade, aproximadamente, de 62%.

Em primeiro lugar, no sentido de atingir este novo estado, ou seja, evoluir do estado atual AS-IS para o estado TO-BE, foram criadas 11 iniciativas, que consistem num conjunto de ações capazes de endereçar uma ou mais oportunidades de melhoria, cobrindo, assim também, um ou mais objetivos organizacionais.

Cada uma das ações de cada iniciativa cobre uma ou controlos e/ou requisitos da norma internacional ISO 27001:2013, e do mesmo modo, também faz uma cobertura de um ou mais artigos do regulamento geral de proteção de dados. O primeiro programa do *roadmap* tem um período de 13 meses e com o conjunto de todas as iniciativas é possível fazer o mapeamento de um total de 52 controlos da ISO, que adicionando os 36 controlos já implementados pela Rangel, perfaz um total de 88 controlos cobertos pelo novo estado futuro. O *roadmap* das iniciativas proporciona, assim, um aumento da cobertura da norma de, aproximadamente, 144%. Consequentemente, para obter uma possível certificação da norma internacional, através de um *Gap Analysis*, determina-se a existência de um défice de 25 controlos que é necessário cobrir, alcançando, assim, um total de 113 controlos cobertos, visto que 1 controlo não é aplicável à atividade da organização.

Em analogia com o RGPD, os controlos já implementados pela Rangel cobrem 16 artigos de um total de 99, e executando todos os planos de ação das iniciativas é possível obter cobertura de mais 22 artigos. Por conseguinte, o novo estado futuro tem uma conformidade de, aproximadamente, 38% (38 artigos mapeados) com o RGPD, verificando, também, um aumento de 138% de cobertura. Além disso, depois do *Gap Analysis* e do programa para a obtenção da certificação da norma, é possível fazer o mapeamento dos artigos que foram cobertos, verificando uma conformidade final com o RGPD de 63% (total de 62 artigos do RGPD). Visto isto, o segundo programa do *roadmap* proporciona um aumento de conformidade de, sensivelmente, 63%.

A primeira conclusão a retirar deste projeto é que adoção de um programa endereçado nas boas práticas de uma norma mundialmente reconhecida para a segurança da informação, é uma forma integrada, coerente e especialmente otimizada para alcanças os objetivos organizacionais do Grupo Rangel: legal, continuidade de negócio, eficiência operacional/financeira e reputacional. Uma alternativa a este programa para a segurança da informação, seria o emparelhamento de forma individual de cada objetivo organizacional, que, muito provavelmente, se distribuiria em 4 programas distintivos, aos quais a soma dos respetivos benefícios seria inferior aos benefícios de um programa integrada para a segurança da informação.

Tal como referido ainda neste capítulo, sendo o objetivo primário da estratégia o aumento, na sua forma geral, do nível de maturidade das tecnologias de informação da Rangel, ao nível da segurança da

informação e não propriamente, a obtenção da certificação da norma ISO 27001:2013, conclui-se também que análise custo-benefício da certificação do final do programa do Roadmap, aponta para a decisão de avançar para a mesma. O final do *Gap Analysis* apresenta um défice de 25 controlos para a certificação, o que representa um custo profundamente pequeno em relação ao ganho reputacional e facilidade de evidenciação da maturidade junto do mercado, com a formalização da certificação. Uma certificação da norma solidificaria posição da Rangel no mercado e também, fortaleceria as relações com os atuais clientes, pelo que, contrariamente, uma perda reputacional e consequentemente, enfraquecimento dessas relações e possível separação através da anulação/não-renovação de contratos, originaria enormes prejuízos para a empresa, como é possível observar na tabela 2.

Adicionalmente, na participação de novos *tenders*, concursos pelos quais é realizada a seleção da melhor empresa que apresente a melhor proposta (na prática, a organização capaz de providenciar os bens ou serviços pelo preço mais barato), uma certificação da norma de segurança de informação providenciaria à Rangel uma grande vantagem competitiva capaz de ser o fator determinante de escolha. Por conseguinte, essa vantagem se traduziria em receita económica, nos valores superiores aos praticados nos contratos atuais (Tabela 2), uma vez que a Rangel estaria a fornecer um serviço mais seguro, ou seja, um serviço de qualidade superior.

Uma outra conclusão a retirar além dos benefícios em cima referidos, o projeto de segurança da informação proporciona à Rangel uma posição forte e uma resposta robusta ao RGPD depois da implementação dos 2 *roadmaps*, temos uma conformidade de, aproximadamente, 63%. A conformidade com o regulamento não é exclusiva apenas a organizações responsáveis pelo tratamento, mas sim a todas que a todas que realizam o algum tratamento de dados pessoais de particulares europeus, por isso, apesar da atividade principal (*core business*) da Rangel não estar assente nesse tratamento, a exposição do mercado e complexidade das operações, obriga à conformidade com o regulamento. Embora o programa conjunto do *Roadmap* não abrange uma cobertura que garante uma conformidade total do regulamento, aumenta, de uma forma excessiva, a capacidade da Rangel Logistics Solutions no cumprimento dos requisitos da mesma.

Efetivamente, um dos maiores obstáculos que o projeto enfrentou foi a tipologia de trabalho, uma vez que o projeto se realizou em teletrabalho durante todo o período da dissertação, devido à pandemia Covid-19. Além disso, após o período de festividades natalícias, o país entrou num segundo confinamento total e, apesar da direção de sistemas de informação já se encontrar em teletrabalho, a necessidade de auxílio a outras LoB, originou uma paragem temporário no projeto de segurança da informação e, consequentemente, ao encurtamento do tempo total para o desenvolvimento do projeto.

Outra limitação sentida foi a falta de compromisso da gestão de topo da organização. Quer a equipa, quer todo o projeto de segurança da informação, é erradamente tabelado com a imagem de dispendioso e não gerador de receita para organização. Além disso, o projeto em si, necessita de muitos recursos, nomeadamente, capital, uma vez que estas tecnologias são de custo elevado, como por exemplo, a instalação de um sistema *anti-malware*, que implementado em toda a organização pode custar facilmente 100 000€; e mão-de-obra qualificada, o que de facto, é dispendioso para a empresa. O retorno deste investimento não sendo fácil de visualizar provoca uma falta de compromisso da gestão de topo, pelo que é contraprodutivo, de modo a alcançar os objetivos organizacionais da Rangel.

Como em qualquer grande projeto envolvendo todos os vértices da empresa, tal como este, o envolvimento de pessoas, tempo estratégico ("timing"), e o compromisso da equipa de liderança são fatores fundamentais para o sucesso. Então, também neste projeto que envolve grandes grupos, é necessário que este se enquadre no plano estratégico da empresa e que toda a equipa de liderança da mesma acredite, e se comprometa a influenciar as respetivas equipas para a conclusão do projeto. Aliado aos fatores referenciados anteriormente, é necessário salientar que mais de 80% dos colaboradores da Rangel, na direção de sistemas de informação, estavam em regime de trabalho remoto durante o período de 2020 e 2021 devido à pandemia covid-19. Circunstâncias essas, atípicas para a empresa que teve de priorizar todos os seus processos, de modo que o impacto na organização fosse nulo. Consequentemente, projetos menos prioritários sofram atrasos devido à escassez de recursos como colaboração e tempo.

Em suma, conclui-se que a pergunta de investigação foi respondida, tendo sido apresentado o *roadmap* (agregação de 2 programas de *roadmap*) para a segurança da informação, pelo que deve ajudar a organização a estar em conformidade com RGPD, a melhorar a sua eficiência operacional e financeira, além do ganho comercial/reputacional.

9.2 Propostas de trabalho futuro

É evidenciado ao longo do projeto de investigação diversos aspetos que, no futuro, devem ser alvo de execução e de consequentemente melhoria.

Após a execução das ações que perfazem o programa conjunto dos Roadmap, é possível a obtenção da certificação da norma ISO 27001:2013, pelo que, como dito em cima, apenas oferece uma reposta robusta ao RGPD. Para a conformidade total do RGPD, é crucial que seja criado um plano de ações, de modo a fazer a cobertura dos restantes 37 artigos do regulamento.

Depois da obtenção da cerificação da norma, é necessário manter e cumprir as ações que fazem parte do plano de monitorização do SGSI, nomeadamente, a realização de avaliações de risco regulares, planos de treino e formação, cumprir o plano de auditorias internas, reavaliações também regulares e entre outras ações. Só deste modo é que se possível manter ter um SGSI funcional e eficaz.

REFERÊNCIAS BIBLIOGRÁFICAS

Accerboni, F., & Sartor, M. (2019). *Quality Management: Tools, Methods, and Standards*.

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

Amorim, A. C., Mira da Silva, M., Pereira, R., & Gonçalves, M. (2021). Using agile methodologies for adopting COBIT. *Information Systems*, *101*, 101496. https://doi.org/10.1016/j.is.2020.101496

Beckers, K., Côté, I., Faßbender, S., Heisel, M., & Hofbauer, S. (2013). A pattern-based method for establishing a cloud-specific information security management system: Establishing information security management systems for clouds considering security, privacy, and legal compliance. In *Requirements Engineering* (Vol. 18, Issue 4). https://doi.org/10.1007/s00766-013-0174-7

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Chaudhuri, A. (2016). Internet of things data protection and privacy in the era of the General Data Protection Regulation. *Journal of Data Protection & Privacy*, *1*(1), 64–75. https://www.ingentaconnect.com/content/hsp/jdpp/2016/00000001/00000001/art00009

de Oliveira Albuquerque, R., García Villalba, L. J., Sandoval Orozco, A. L., de Sousa Júnior, R. T., & Kim, T. H. (2016). Leveraging information security and computational trust for cybersecurity. *Journal of Supercomputing*, *72*(10), 3729–3763. https://doi.org/10.1007/s11227-015-1543-4

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls. *Information and Computer Security*, *28*(4), 645–662. https://doi.org/10.1108/ICS-01-2020-0004

Disterer, G. (2013). *ISO / IEC 27000 , 27001 and 27002 for Information Security Management*. *2013*(April), 92–100.

Eicher, L. D., Kuert, W., Maréchal, R., Grey, V., Frontard, R., Sturen, O., Thor, A., & Barchietto, R. (1997). *Recollections from ISO ' s first fifty years*. http://www.iso.org/iso/home/about/the_iso_story.htm

En, N. P. (2015). *No orm ma Po ortu ugu uesa a*.

Ferreira, C., Nery, A., & Pinheiro, P. R. (2016). A Multi-Criteria Model in Information Technology Infrastructure Problems. *Procedia Computer Science*, *91*(December), 642–651. https://doi.org/10.1016/j.procs.2016.07.161

Gomes, J. (2018). *Information System Maturity Models in Healthcare*.

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, *11*(1), 55–61. https://doi.org/10.1016/j.istr.2005.12.004

Hjerppe, K., Ruohonen, J., & Leppänen, V. (2019). The general data protection regulation: Requirements, architectures, and constraints. *Proceedings of the IEEE International Conference on Requirements Engineering*, *2019-September*, 265–275. https://doi.org/10.1109/RE.2019.00036

Hochstein, A. (2005). *Service Oriented IT Management : Benefit , Cost and Success Factors*.

Iden, J., & Eikebrokk, T. R. (2013). Implementing IT Service Management: A systematic literature review. *International Journal of Information Management*, *33*(3), 512–523. https://doi.org/10.1016/j.ijinfomgt.2013.01.004

ISACA. (2012). Enabling Processes. In *Cobit 5*.

Kerr, D. S., & Murthy, U. S. (2013). The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey. *Information and Management*, *50*(7), 590–597. https://doi.org/10.1016/j.im.2013.07.012

Kurnianto, A., Isnanto, R., & Widodo, A. P. (2018). Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs. *E3S Web of Conferences*, *31*, 0–5. https://doi.org/10.1051/e3sconf/20183111013

Larrocha, E. R., Minguet, J. M., Díaz, G., Castro, M., & Vara, A. (2010). Filling the gap of Information Security Management inside ITIL®: Proposals for posgraduate students. *2010 IEEE Education Engineering Conference, EDUCON 2010*, 907–912. https://doi.org/10.1109/EDUCON.2010.5492480

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. *Journal of Information Systems Engineering & Management*, *4*(2), 2–9. https://doi.org/10.29333/jisem/5888

Mahy, Y., Ouzzif, M., & Bouragba, K. (2017). Supporting ITIL processes implementation using business process management systems. *Proceedings - 2016 3rd International Conference on Systems of Collaboration, SysCo 2016*, 31–34. https://doi.org/10.1109/SYSCO.2016.7831338

Management, I. (n.d.). *IT GOVERNANCE IN DIGITAL TRANSFORMATION A COBIT 5 overview according IDC Maturityscape Ana Catarina Saldanha Jerónimo*.

Mark Saunders, Philip Lewis, A. T. (2012). Research methods for business students. In *International Journal of the History of Sport* (Vol. 30, Issue 1). https://pdfcoffee.com/research-methods-for-business-students-7th-edition-2015-mark-n-k-saunders-philip-lewis-adrian-thornhill-pdf-free.html

McNaughton, B., Ray, P., & Lewis, L. (2010). Designing an evaluation framework for IT service management. *Information and Management*, *47*(4), 219–225. https://doi.org/10.1016/j.im.2010.02.003

Nabil Almunawar, M., Susanto, H., & Chee Tuan, Y. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences IJECS-IJENS*, *11*.

O'Brien, R. (1998). An overview of the methodological approach of action Research. *University of Toronto*, 1–15.

Othman, M., Ahmad, M. N., Suliman, A., Arshad, N. H., & Maidin, S. S. (2014). COBIT principles to govern flood management. *International Journal of Disaster Risk Reduction*, *9*, 212–223. https://doi.org/10.1016/j.ijdrr.2014.05.012

Ozdemir, Y., Basligil, H., Alcan, P., & Kandemirli, B. M. (2014). *Evaluation and Comparison of Cobit , Itil and Iso27K1 / 2 Standards Within the*. *11*(11), 22–24.

PMI. (2017). *Agile Practice Guide* (Project Management Institute (ed.); First Edit). Project Management Institute, Inc.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), 1–20. https://doi.org/10.1093/cybsec/tyy001

Pollard, C., & Cater-Steel, A. (2009). Justifications, strategies, and critical success factors in successful ITIL implementations in U.S. and Australian companies: An exploratory study. *Information Systems Management*, *26*(2), 164–175. https://doi.org/10.1080/10580530902797540

Qusef, A., Arafat, M., & Al-Taher, S. (2018). Organizational management role in information security management system. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3231053.3231064

Rezakhani, A., Hajebi, A., & Mohammadi, N. (2011). Standardization of all Information Security Management Systems. *International Journal of Computer Applications*, *18*(8), 4–8. https://doi.org/10.5120/2307-2592

Samonas, S., & Coss, D. (2014). The CIA strikes back: redefining confidentiality, integrity and availability in security. *Journal of Information System Security - JISSec*, *10*(3), 21–45. www.jissec.org

Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian Journal of Science and Technology*, *5*(2), 2170–2176. https://doi.org/10.17485/ijst/2012/v5i3.1

Sirur, S., Nurse, J. R. C., & Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). *Proceedings of the ACM Conference on Computer and Communications Security*, *iii*, 88–95. https://doi.org/10.1145/3267357.3267368

Tan, W.-G., Cater-Steel, A., Toleman, M., & Seaniger, R. (2007). Association for Information Systems AIS Electronic Library (AISeL) Implementing Centralised IT Service Management: Drawing Lessons from the Public Sector. *Acis 2007*, 10. http://aisel.aisnet.org/acis2007

Tan, W. G., Cater-Steel, A., & Toleman, M. (2009). Implementing it service management: A case study focussing on critical success factors. *Journal of Computer Information Systems*, *50*(2), 1–12. https://doi.org/10.1080/08874417.2009.11645379

Taylor, G., & East. (2013). Running Head: Itil V3 Improves Information Security Management. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers and Security*, *24*(2), 99–104. https://doi.org/10.1016/j.cose.2005.02.002

Wegmann, A., Regev, G., Garret, G. A., & Maréchal, F. (2008). Specifying services for ITIL service management. *2008 International Workshop on Service-Oriented Computing: Consequences for Engineering Requirements, SOCCER'08*, 8–14. https://doi.org/10.1109/SOCCER.2008.7

Zafar, H., Ko, M. S., & Osei-Bryson, K. M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers*, *18*(6), 1205–1215. https://doi.org/10.1007/s10796-015-9562-5

APÊNDICE 1 – COMPARAÇÃO ENTRE O ESTADO ATUAL AS-IS E O ESTADO FUTURO TO-BE

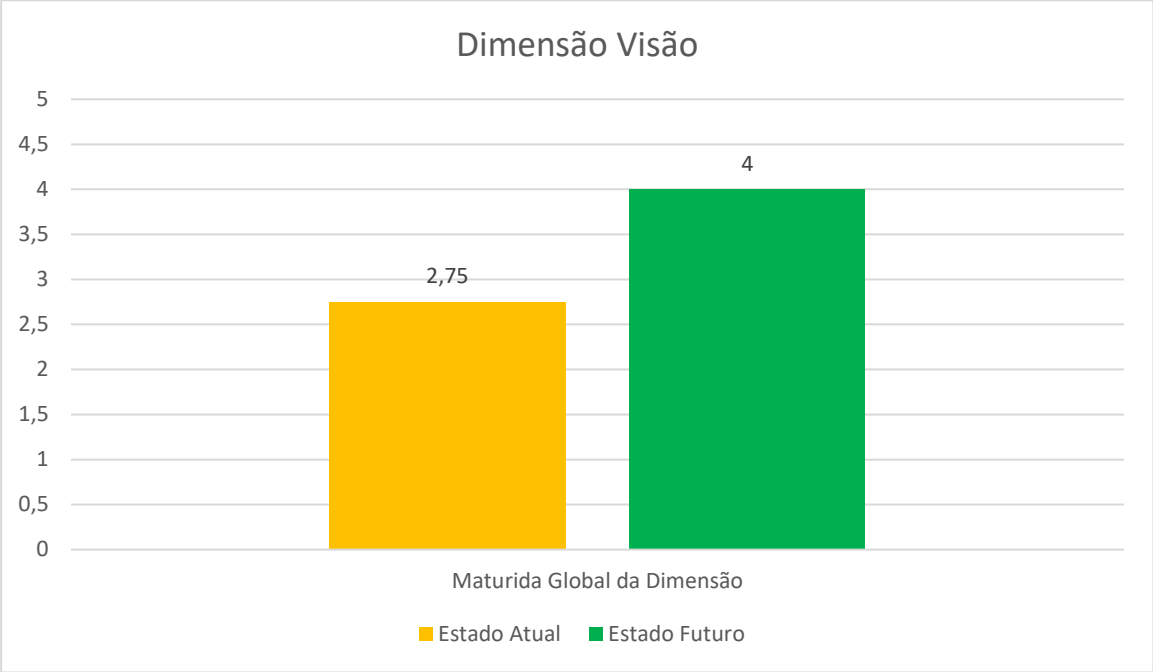


Figura 36 – Comparação do estado de maturidade global entre o estado atual e o estado futuro da dimensão Visão

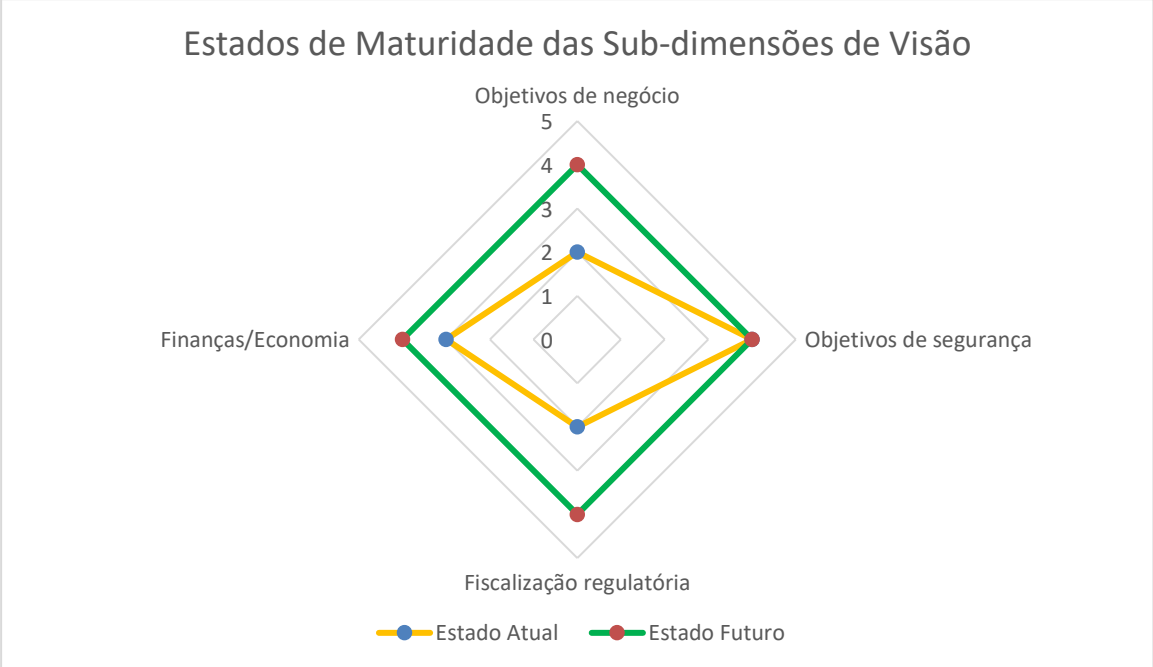


Figura 37 – Comparação entre o estado atual e o estado futuro para as subdimensões da dimensão Visão

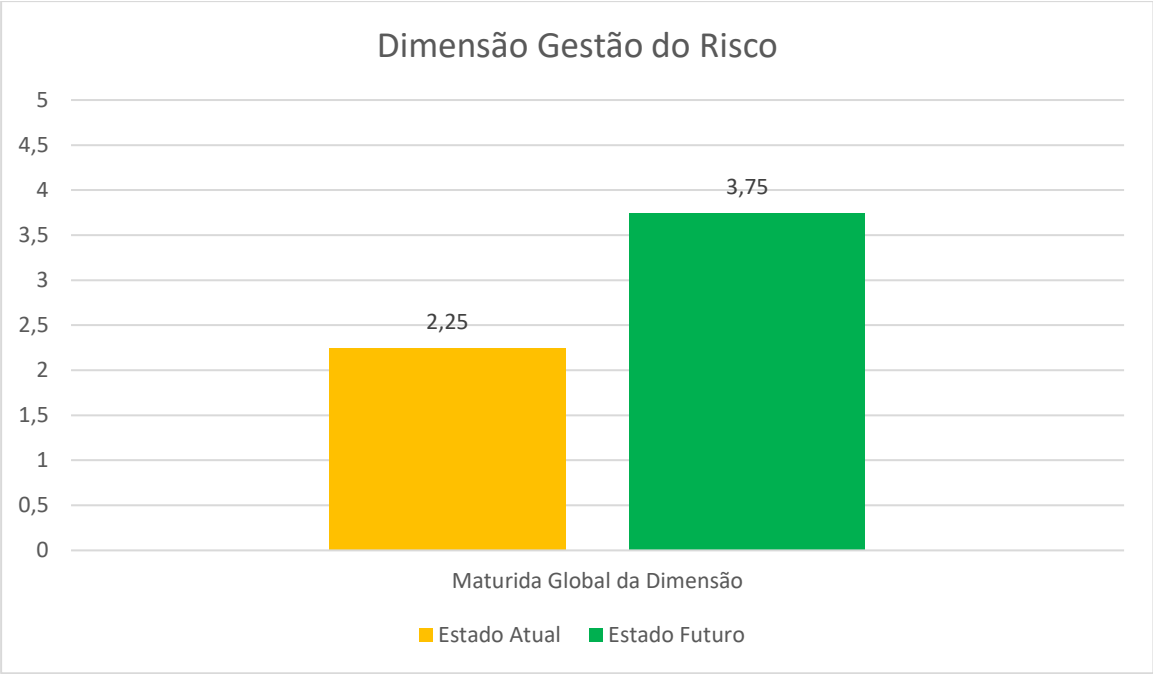


Figura 38 - Comparação do estado de maturidade global entre o estado atual e o estado futuro da dimensão Gestão do Risco

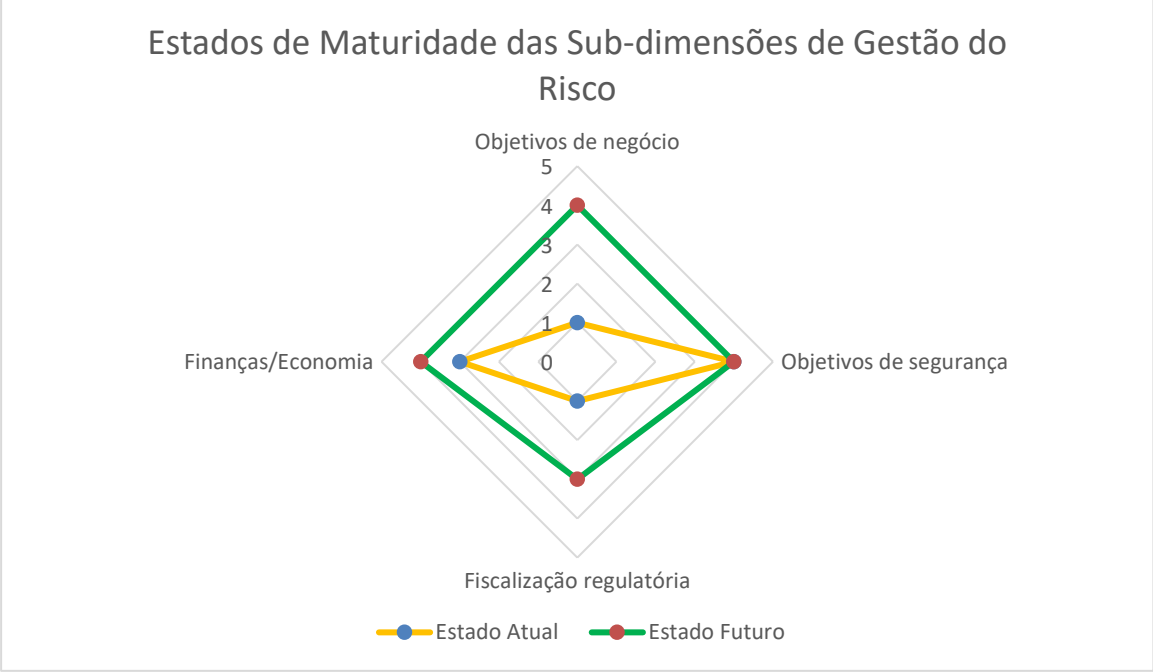


Figura 39 – Comparação entre o estado atual e o estado futuro para as subdimensões da dimensão Gestão do Risco

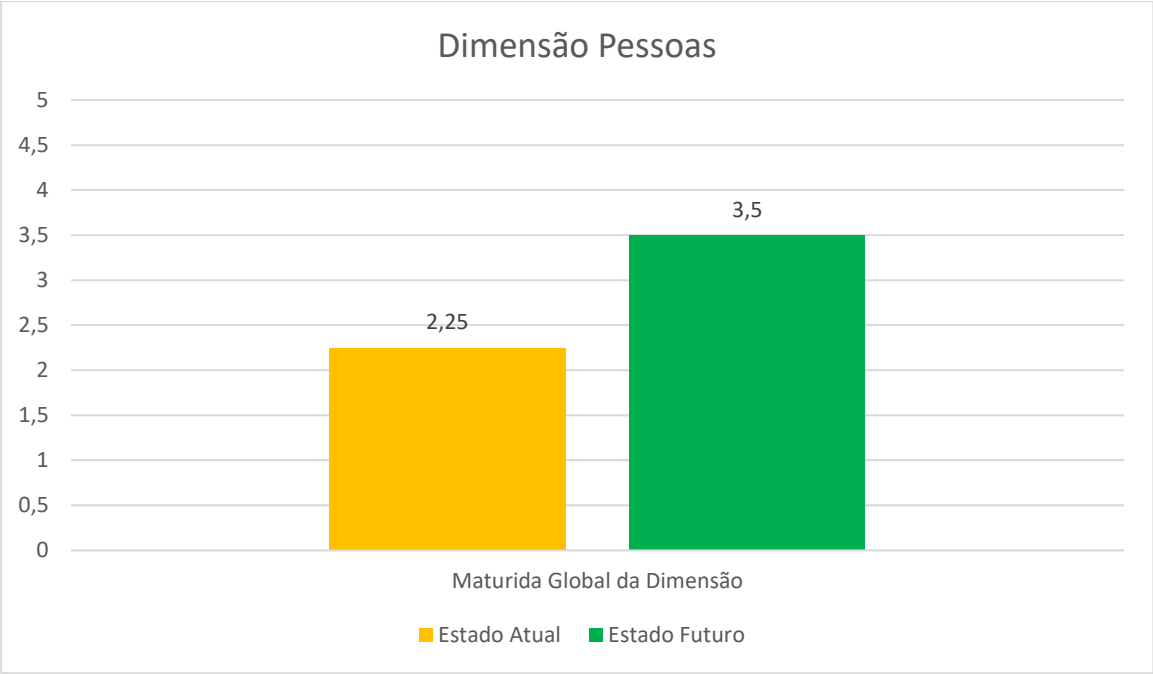


Figura 40 - Comparação do estado de maturidade global entre o estado atual e o estado futuro da dimensão Pessoas

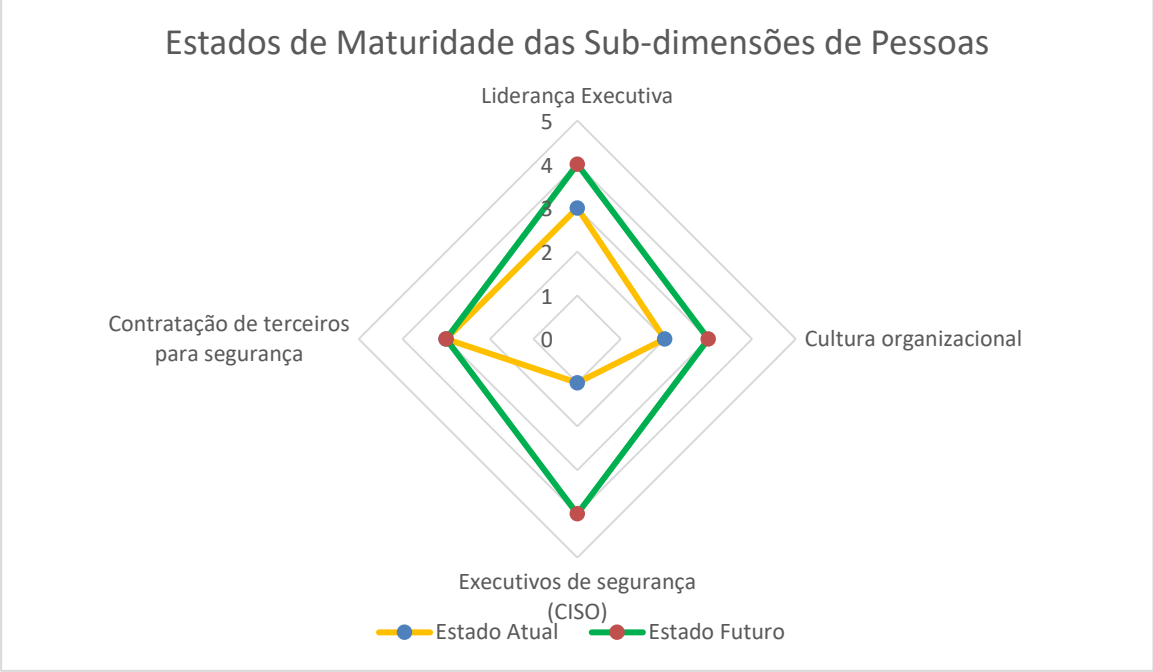


Figura 41 – Comparação entre o estado atual e o estado futuro para as subdimensões da dimensão Pessoas

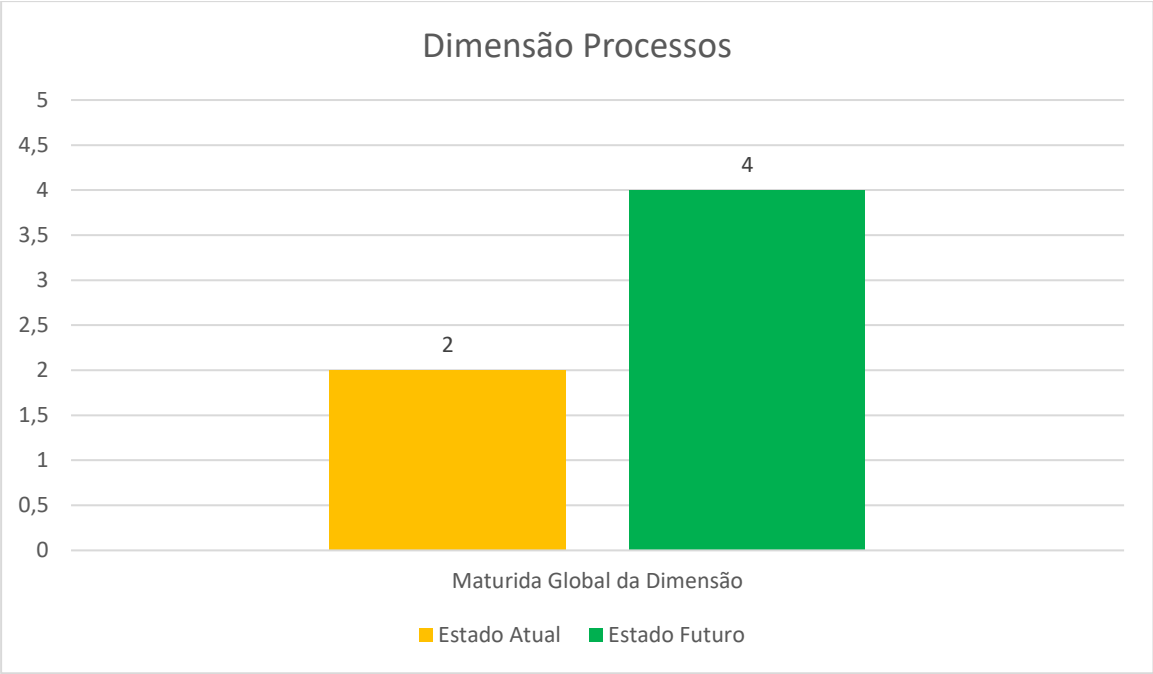


Figura 42 – Comparação do estado de maturidade global entre o estado atual e o estado futuro da dimensão Processos

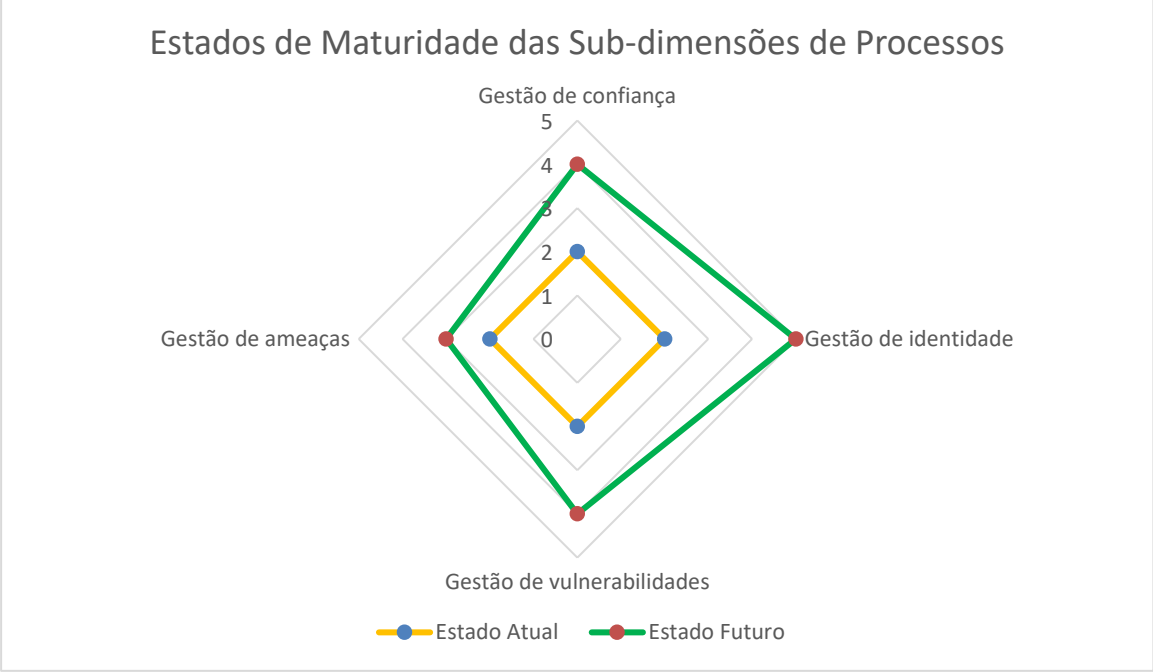


Figura 43 – Comparação entre o estado atual e o estado futuro para as subdimensões da dimensão Processos

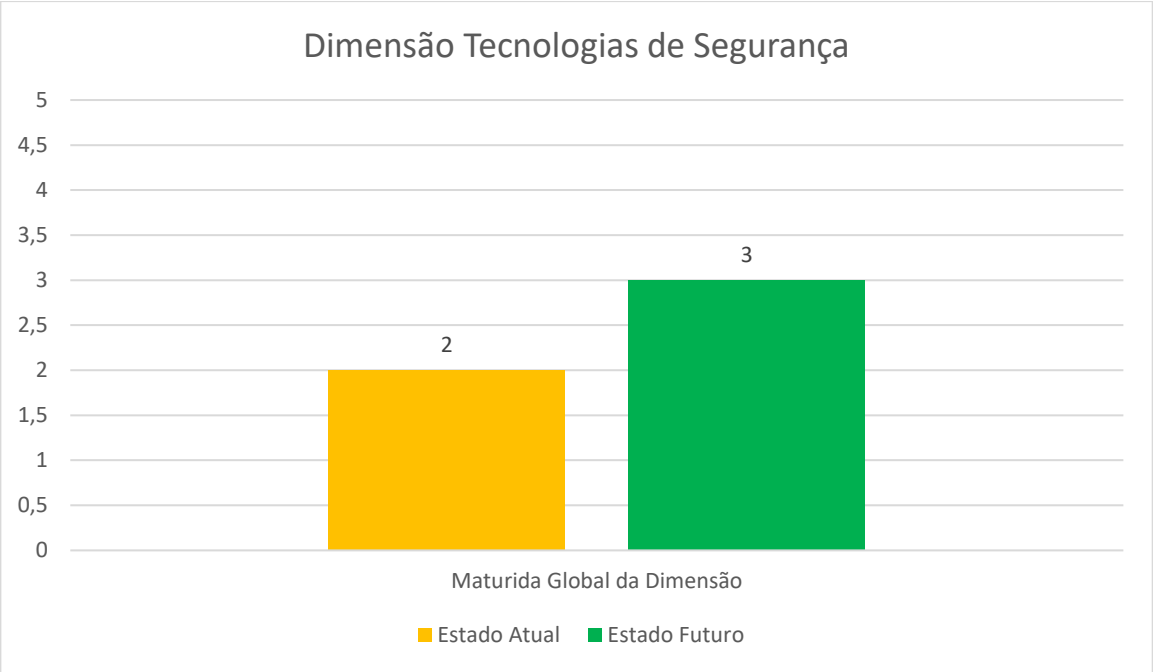


Figura 44 – Comparação do estado de maturidade global entre o estado atual e o estado futuro da dimensão Tecnologias de Segurança

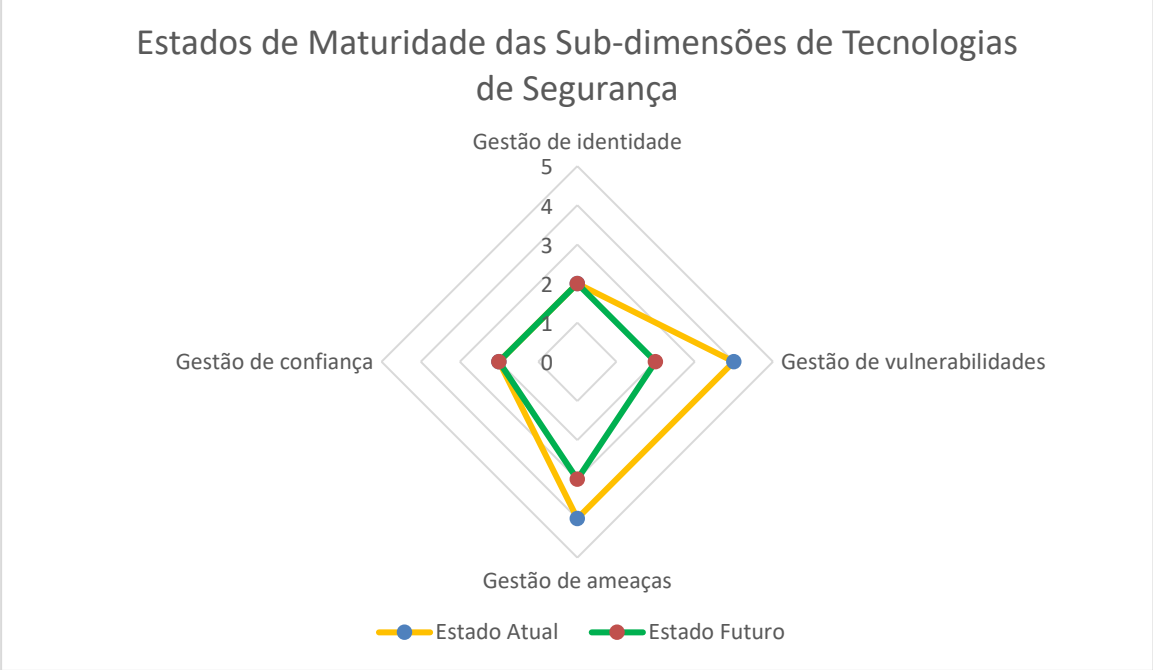


Figura 45 – Comparação entre o estado atual e o estado futuro para as subdimensões da dimensão Tecnologias de Segurança

APÊNDICE 2 – POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA

Rangel

Política de Privacidade, Proteção de Dados e Segurança

DPO.POL.001/0

Página: 1 de 7

1. Objetivo

Regular o tratamento de dados pessoais, descrevendo assim como a Rangel Logistics Solutions pretende garantir a conformidade da sua atuação com o Regulamento Geral de Proteção de Dados e a demais legislação aplicável em matéria de privacidade e proteção de dados.

2. Definições

Dados pessoais – informação relativa a uma pessoa singular identificada ou identificável, como um identificador ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

Atividade de tratamento – operação ou conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados, tais como recolha, registo, organização, estruturação, conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, limitação, apagamento ou destruição.

Responsável pelo Tratamento (data controller) – pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e meios de tratamento dos dados pessoais. Por exemplo, a Rangel Logistics Solutions quando trata dados pessoais dos seus trabalhadores ou dos representantes dos seus clientes.

Subcontratante (data processor) – pessoa singular ou coletiva, autoridade pública, agência ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento detestes. Por exemplo, a Rangel Logistics Solutions quando trata dados pessoais por conta dos seus Clientes no âmbito da prestação de serviços de distribuição e transporte.

Titular de dados – pessoa singular cujos dados são recolhidos e tratados. Por exemplo, os trabalhadores da Rangel Logistics Solutions ou os clientes finais dos clientes Rangel.

Destinatário – pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo a quem sejam comunicados dados pessoais, independentemente de se tratar ou não de um terceiro. Por exemplo, a Autoridade Tributária ou as Transportadoras contratadas pelos clientes da Rangel Logistics Solutions.

Violação de dados pessoais – violação da segurança que provoque, de modo acidental ou ilícito, (i) a perda ou utilização injustificada (por qualquer meio) de dados pessoais, (ii) o tratamento, divulgação, acesso, alteração, corrupção, transferência, venda, aluguer, destruição ou utilização involuntária, não autorizada e/ou ilícita de dados pessoais ou (iii) qualquer outra ação ou omissão que comprometa ou possa comprometer a segurança, confidencialidade, ou integridade de dados pessoais. Por exemplo, o envio de um e-mail que contenha dados pessoais para o destinatário errado.

Confidencialidade – propriedade que limita o acesso a informação tão somente às entidades legitimas, ou seja, àquelas autorizadas pelo proprietário da informação.

Integridade – propriedade que garante a informação manipulada mantém todas as características originais estabelecidas pelo proprietário da informação, incluindo controlo de mudanças e garantia do seu ciclo de vida.

Disponibilidade – propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles utilizadores autorizados pelo proprietário da informação.

3. Princípios

Na recolha e tratamento de dados pessoais, os colaboradores da Rangel Logistics Solutions devem respeitar os seguintes princípios:

Licitude, Lealdade e Transparência – Apenas recolher e tratar dados pessoais quando exista fundamento legal para o efeito e assegurando sempre que o titular de dados é informado sobre as atividades de tratamento de dados pessoais realizadas.

Limitação das finalidades – Apenas recolher dados pessoais para finalidades previamente determinadas, explícitas e legítimas, não podendo estes dados pessoais ser tratados posteriormente de uma forma incompatível com essas finalidades.

Minimização – Apenas recolher os dados pessoais absolutamente necessários e adequados às finalidades para as quais são tratados, garantindo ainda que os mesmos estarão apenas acessíveis ao conjunto de colaboradores que carecem de acesso aos mesmos para o exercício das suas funções.

Exatidão – Garantir que os dados pessoais recolhidos são exatos e mantêm-se atualizados, devendo, sempre que necessário, adotar as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora.

Limitação da conservação – Garantir que os dados pessoais são conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados.

Elaborado:	Data:	Aprovado:	Data:

Entrada em vigor:

DGSI.MOD.001/0

Figura 46 - Política de Privacidade, proteção de dados e segurança (página 1/7)

APÊNDICE 3 – INSTRUÇÕES DE TRABALHO – AÇÃO COMPLEMENTAR PARA A INICIATIVA Nº1

Na Figura 47, 48 e 49 está representado a instrução de trabalho "*Onedrive* e Cópias de Segurança".

Rangel LOGISTICS SOLUTIONS

Instrução de Trabalho

Onedrive e Cópias de segurança

Página: 1 de 3

1. **Objetivo**

Descrever os passos/instruções de ativação do Onedrive, bem como a ativação das cópias de segurança e acesso à Reciclagem para a recuperação de ficheiros apagados.

2. **Âmbito**

Salvaguarda de toda a informação do Grupo Rangel.

3. **Responsabilidades**

Técnicos de Suporte e Coordenador de Infraestruturas de IT
Todos os colaboradores da *Rangel Logistics Solutions* que utilizadores da plataforma *Microsoft Teams*

4. **Definições**

Onedrive: local de armazenagem de documentos pessoais na *cloud*, funcionando assim como repositório pessoal.
Back-up/Cópia de segurança: é a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver eliminação acidental ou corrupção de dados.

5. **Modo de Proceder**

Cumprindo as normas de Segurança da Informação, todos os colaborados do grupo Rangel devem armazenar os ficheiros com informação de negócio *Onedrive* com a ativação de cópias de segurança das principais: **Ambiente de Trabalho, Documentos e Imagens**. Este medida tem como fim o desuso do armazenamento local de documentos de trabalho.

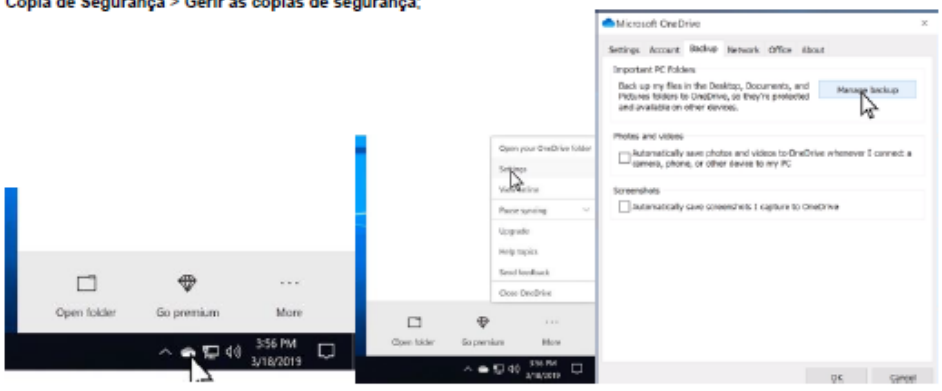
Ativação do Onedrive

A cada colaborador da Rangel é atribuído uma conta empresarial associada a uma conta licenciada Microsoft 365, já com uma *cloud* de armazenamento *OneDrive*. O colaborador pode armazenar qualquer ficheiro relacionado com o negócio, a partir de qualquer dispositivo eletrónico associado à sua conta, estando apenas disponível para si. Contudo, também pode partilhar esses ficheiros e pastas OneDrive com os restantes colaboradores.

Ativação de cópias de segurança

De modo a podermos ter os ficheiros de negócio salvaguardados em caso de incidentes, que porventura, podem levar à perda dessa mesmo informação, é possível ativar e gerir a cópia de segurança do **Onedrive**.

1. Selecione o ícone de nuvem azul na área de notificação do Windows, selecione **Ajuda & Definições** > **Definições** e, em seguida, **Cópia de Segurança** > **Gerir as cópias de segurança**;



2. Selecione as pastas das quais você deseja fazer cópia de segurança;
3. Selecione **Iniciar Cópia de Segurança**;

Elaborado: José Luís Alves **Data: ___/___/____** **Aprovado:** **Data: ___/___/____**

Entrada em vigor: ___/___/____

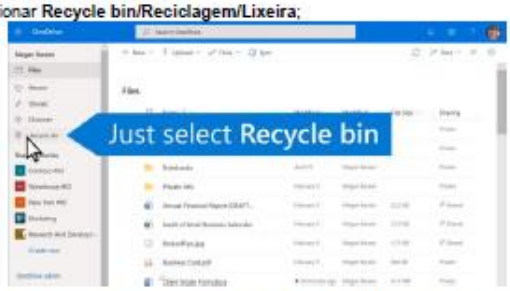
Figura 47 - Instrução de Trabalho "*Onedrive* e Cópias de Segurança" (página 1/3)

Recuperação de ficheiro apagados

Se muitos dos seus ficheiros do OneDrive tiverem sido eliminados, substituídos, danificados ou infetados por software maligno, pode restaurar o seu OneDrive completo para uma data anterior. Além disso, o Restauro de Ficheiros ajuda os utilizadores a anular todas as ações que ocorreram em ficheiros e pastas durante os últimos 30 dias.

Tendo o utilizador conetado a sua conta no website da Onedrive:

1. No painel de navegação, selecionar **Recycle bin/Reciclagem/Lixeira**;

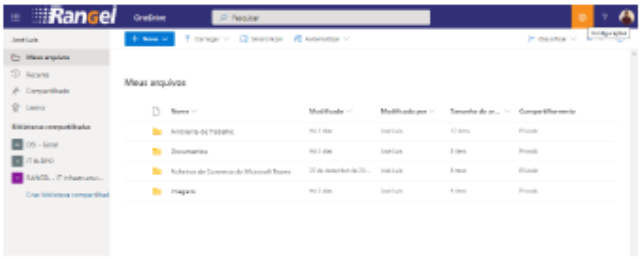


2. Selecionar os ficheiros ou pastas que se pretende restaurar apontando para cada item e clicar na caixa de verificação de círculos que aparece e, em seguida, clicar em **Restaurar**;

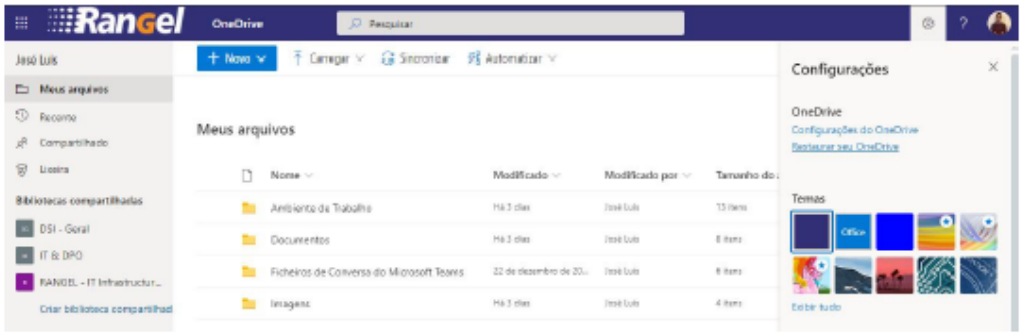
Ou através de um processo também simples:

1. Selecionar o ícone **Configurações** (na figura abaixo, destacado a laranja no canto superior direito);

Figura 48 - Instrução de Trabalho "*Onedrive* e Cópias de Segurança" (página 2/3)



2. De seguida, selecionar a opção **Restaurar seu OneDrive**;



3. Por fim, selecionar a data até o qual pretende restaurar o seu *OneDrive*, preferencialmente, até a última atualização antes do incidente que despoletou essa restauração, e depois clicar **Restaurar**;

Figura 49 - Instrução de Trabalho "*Onedrive* e Cópias de Segurança" (página 3/3)

Nas Figuras 50, 51 e 52, está representada a Instrução de trabalho "Verificação das Condições de Segurança da Informação na Partilha de Links e Emails".

Rangel

Instrução de Trabalho

Verificação das Condições de Segurança da Informação na Partilha de Links e Emails

Página: 1 de 3

1. **Objetivo**

Descrever os passos/instruções na partilha de documentos através do OneDrive entre os colaboradores do Gruo Rangel, juntamente dos cuidados a ter em conta, de forma a cumprir as regras de segurança da informação.

2. **Âmbito**

Salvaguarda de toda a informação do Grupo Rangel.
Cumprir e estar em conformidade com o Regulamento Geral de Proteção de Dados.

3. **Responsabilidades**

Todos os colaboradores do Grupo *Rangel Logistics Solutions*.

4. **Definições**

Onedrive: local de armazenagem de documentos na *cloud*, funcionando assim como repositório pessoal.
E-mail: Sistema de transmissão de mensagens escritas de um computador para outro computador (ou dispositivo eletrónico), via Internet ou através de outras redes de computadores;
Link: é a "ligação" ou "endereço" de um documento (ou um recurso) na *World Wide Web*.

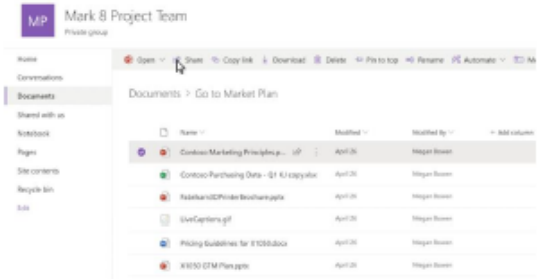
5. **Modo de Proceder**

Muitos dos perigos e ameaças à segurança da informação, passam por violações internas e erro humano, através de envio de informação contendo dados pessoais ou informação sensível de negócio para terceiros. A partilha de informação para um destinatário errado, mesmo não sendo intencional, é considerado um acidente e uma violação de dados. De forma a proteger os dados pessoais e informação crítica de negócio, é da responsabilidade de cada colaborador da Rangel adotar regras de segurança, tanto na verificação de e-mails, como na partilha de links entre colaboradores.

Esta partilha de ficheiros pode ser realizada de várias formas: diretamente através do Portal Online da sua conta OneDrive, diretamente de aplicações do Office 365 como Word, PowerPoint, Excel, entre outros, diretamente do Explorador de ficheiros do seu computador (desde que o OneDrive esteja ativo) ou ainda, através do OneDrive Mobile Apps.

Todo as opções de partilha funcionam sobre o mesmo mecanismo (por defeito, vai ser descrita o modo de partilha através do Portal Online OneDrive).

1. Aceda ao website do OneDrive e inicie sessão com a sua conta de domínio da Rangel.
2. Selecione o ficheiro ou pasta que pretende partilhar ao selecionar o círculo respondente desse ficheiro ou pasta a partilhar.
3. Selecione **Partilhar** na parte superior da página.

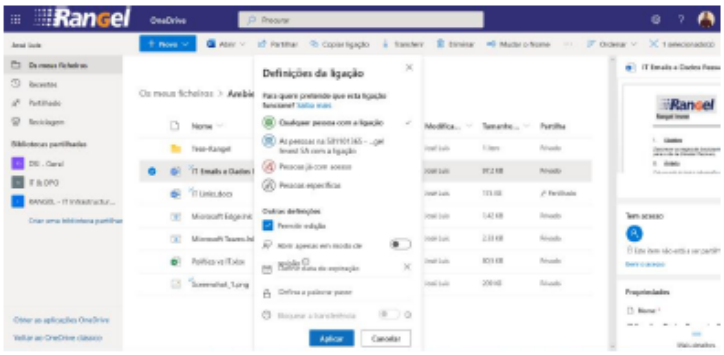


4. Por definição, a opção pre-definida de ligação é: "Qualquer pessoa com a ligação", onde depois pode definir as opções pretendidas na sua ligação e, em seguida, selecione **Aplicar** quando tiver terminado.

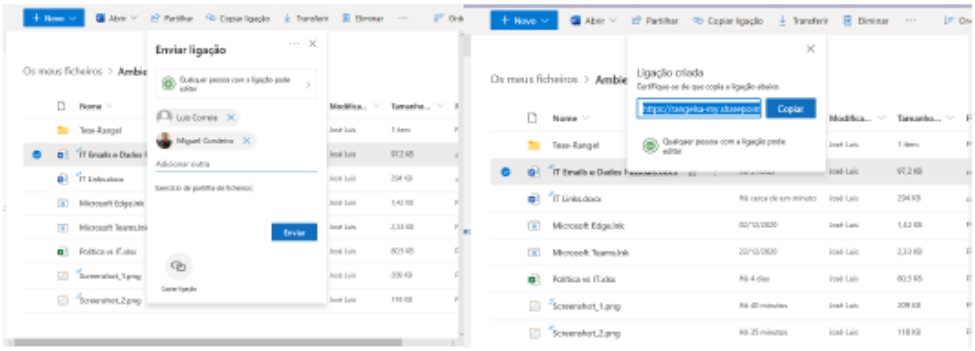
- **Permitir a edição** - outros colaboradores podem editar ficheiros e adicionar ficheiros numa pasta partilhada. Os destinatários podem reencaminhar a ligação, alterar a lista de pessoas que partilham os ficheiros ou a pasta e alterar as permissões dos destinatários. Se estiver a partilhar uma pasta, as pessoas com permissões de Edição podem copiar, mover, editar, mudar o nome, partilhar e eliminar qualquer coisa dentro da pasta.
- **Definir data de expiração** - A ligação só irá funcionar até à data que definiu. Após essa data, a ligação será inválida e terá de criar uma nova ligação para os utilizadores que precisem de acesso ao seu ficheiro ou pasta.
- **Definir palavra-passe** - Quando um utilizador clicar na ligação, ser-lhe-á pedido para introduzir uma palavra-passe antes de poder aceder ao ficheiro. Terá de fornecer a sua palavra-passe de forma **separada** aos utilizadores.

Elaborado: José Luís Alves **Data: ___/___/____** **Aprovado:** **Data: ___/___/____**

Figura 50 - Instrução de Trabalho "Verificação das Condições de Segurança da Informação na Partilha de Links e Emails" (página 1/3)



5. Insira os endereços de e-mail das pessoas com quem gostaria de partilhar e adicione uma mensagem opcional, enviando assim a ligação por e-mail ou também se pode selecionar em **Copiar ligação**, um link é gerado e depois selecionar **Copiar**, podendo colar esse link numa conversa ou noutra plataforma digital.



Nota: O OneDrive tem predefinido a opção de ligação "Qualquer pessoa com a ligação", no entanto têm outras opções pra restringir o nível de acesso.

- A opção **Qualquer pessoa** dá acesso a todas as pessoas que receberem a ligação, quer a tenham recebido diretamente de si ou lhes tenha sido reencaminhada por outro utilizador. Isto poderá incluir pessoas fora da sua organização.
- A opção **Pessoas na <A Sua Organização>** dá acesso ao ficheiro a todas as pessoas na sua organização que tenham a ligação, quer a tenham recebido diretamente de si ou lhes tenha sido reencaminhada por outro utilizador.
- **Pessoas já com acesso** pode ser utilizado por pessoas que já têm acesso ao documento ou pasta e não altera as permissões no item. Utilize esta opção se quiser enviar uma ligação a alguém que já tem acesso.
- A opção **Pessoas específicas** dá acesso apenas às pessoas que especificar, no entanto, outras pessoas poderão já ter acesso. Se as pessoas reencaminharem o convite de partilha, apenas as pessoas que já têm acesso ao item poderão utilizar a ligação.

Figura 51 - Instrução de Trabalho "Verificação das Condições de Segurança da Informação na Partilha de Links e Emails" (página 2/3)

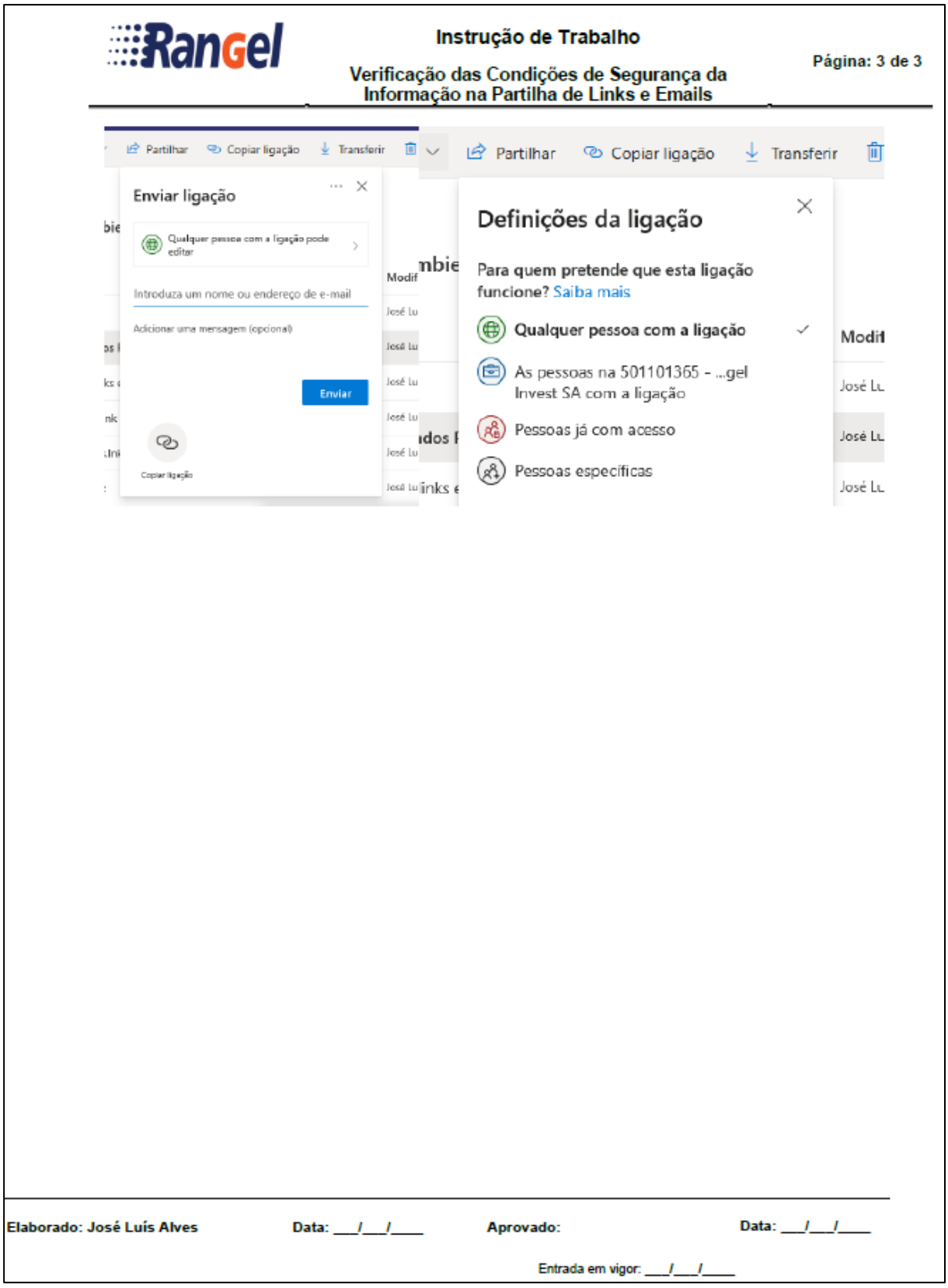


Figura 52 - Instrução de Trabalho "Verificação das Condições de Segurança da Informação na Partilha de Links e Emails" (página 3/3)

APÊNDICE 4 – PROCEDIMENTO DE COMUNICAÇÃO NUMA VIOLAÇÃO DE DADOS

Rangel | **Procedimento** | DPO.PG.004/0

Gestão de violação de dados pessoais | Página: 1 de 2

1. **Objetivo**

Estabelecer as regras para a gestão de incidentes que configuram violações de dados.

2. **Responsabilidades**

As responsabilidades pelo cumprimento do determinado no Procedimento estão definidas no Ponto 4., na coluna "Responsável".

3. **Definições**

Dados pessoais – informação relativa a uma pessoa singular identificada ou identificável, como um identificador ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

Violação de dados pessoais – violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

4. **Modo de Proceder**

Ação	Descrição Sumária	Responsável	Documentos Registos
Comunicação de Incidente	O Utilizador que detete a possível violação de dados deve reportar de imediatamente a ocorrência à Equipa de infraestruturas, através da helpdesk do Sistema de gestão de incidents. Por sua vez, a equipa de infraestruturas imediatamente informa o DPO (telefone).	Utilizador que apure a possível ocorrência de violação de dados. Equipa de infraestruturas	Registo no helpdesk
Análise de risco e avaliação de responsabilidade	No prazo de 24h após a detação do incidente, o DPO e a equipa de infraestruturas analisam em conjunto a ocorrência, tendo em consideração os dados pessoais potencialmente visados, o tipo de violação de segurança, as medidas técnicas e organizativas implementadas à data e os destinatários envolvidos. Nesta fase, emite o seu parecer sobre a responsabilidade da organização pela violação de dados, bem como se a violação é suscetível de causar risco para os titulares de dados.	DPO e equipa de infraestruturas	Relatório E-mail
Comunicação ao CA e Country Managers	No prazo de 12h após a conclusão da análise, o DPO comunica ao CA e Country Manager (se aplicável) a ocorrência da violação de dados e o resultado da análise de risco e responsabilidade efetuada, emitindo o seu parecer sobre a necessidade de informar o Responsável pelo Tratamento (se aplicável), bem como sobre a obrigatoriedade de notificar a CNPD e os titulares de dados.	DPO	Ata de reunião E-mail Relatório

Figura 53 - Procedimento de comunicação em caso de uma violação de dados (página 1/2)

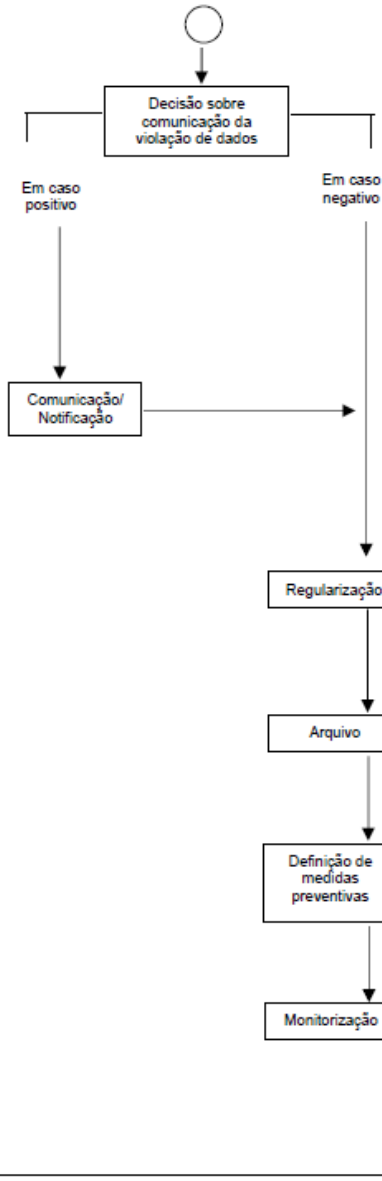
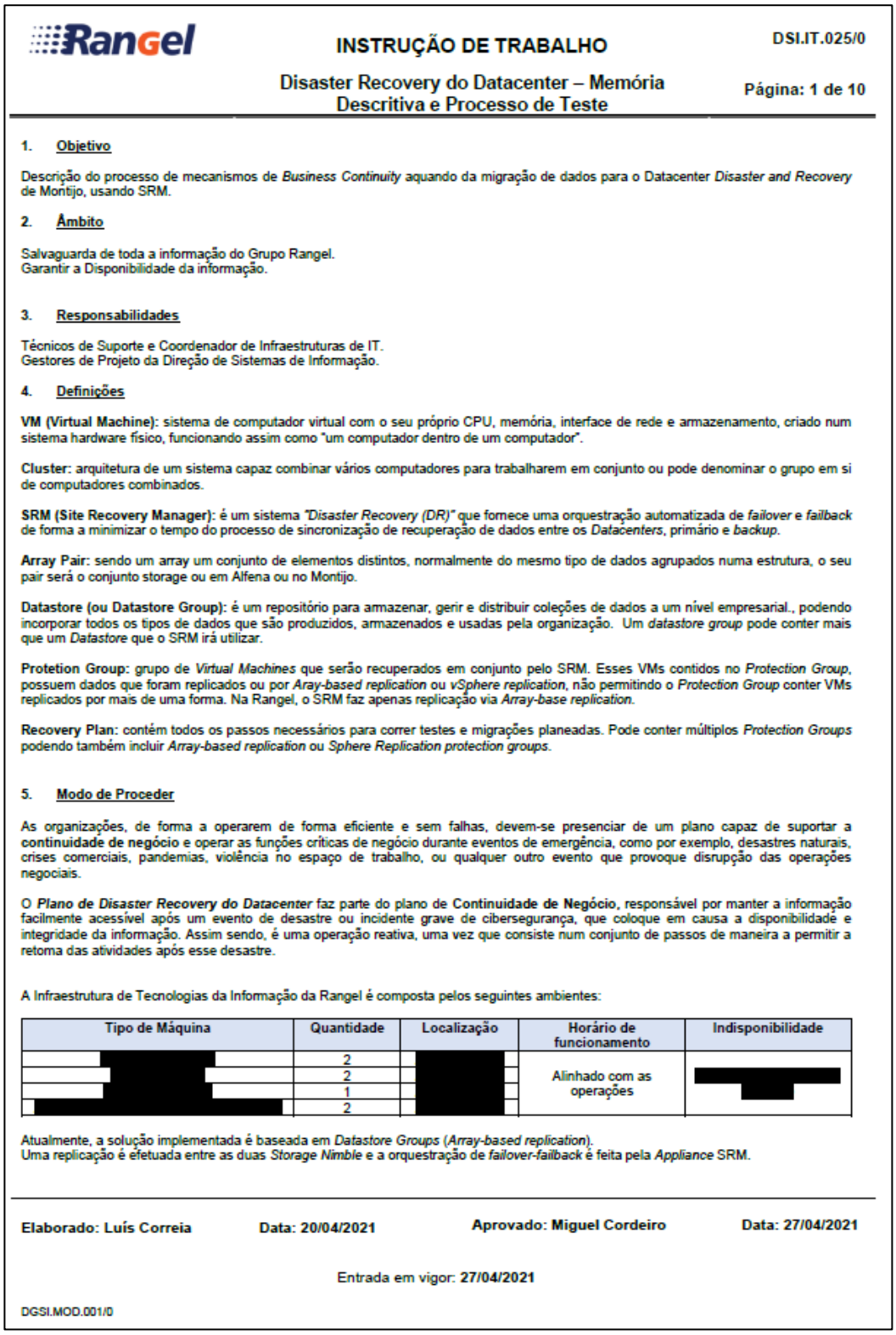
Ação	Descrição Sumária	Responsável	Documentos Registos
	No prazo de 12h após receção do parecer do DPO, o CA e o Country Manager (se aplicável) decidem sobre: a) Comunicar ao Responsável pelo Tratamento a ocorrência de violação de dados (se aplicável) b) Notificar a CNPD e/titulares de dados (no caso da organização atuar coom Responsável pelo Tratamento) No prazo de 12h após a decisão do CA, prestando todas as informações exigidas por lei ou contrato, o DPO informa, consoante aplicável: - Responsável pelo Tratamento - CNPD - Titulares de Dados Os responsáveis definem e executam as medidas de reparação da violação com vista a eliminar/mitigar os seus eventuais efeitos negativos. O DPO arquiva o relatório, bem como toda a correspondência e demais evidências relativas à violação de dados. Os responsáveis definem medidas de prevenção (e prazos de execução) de futuras violação de dados. No final de cada ano, os responsáveis elaboram um relatório com vista a analisar quantitativa e qualitativamente os incidentes ocorridos, bem como a documentar o cumprimento das medidas preventivas definidas.	CA Country Manager DPO DPO, IT, Direções consoante aplicável DPO DPO, Direção de IT, Outras Direções consoante aplicável DPO, Direção de IT, Outras Direções (se aplicável)	Ata de reunião E-mail Relatório E-mail Plataforma designada para o efeito Relatório Relatório Ata E-mails Relatório Anual

Figura 54 - Procedimento de comunicação em caso de uma violação de dados (página 2/2)

APÊNDICE 5 – INSTRUÇÃO DE TRABALHO PARA O PLANO DE CONTINUIDADE DE NEGÓCIO

Neste apêndice, são apresentadas as instruções de trabalho para a continuidade de negócio. Na Figura 55 está representado o Disaster Recovery do Datacenter. Por motivos de confidencialidade, apenas é apresentado a primeira página de um total de 10.



Rangel

INSTRUÇÃO DE TRABALHO — DSI.IT.025/0

Disaster Recovery do Datacenter – Memória Descritiva e Processo de Teste — Página: 1 de 10

1. **Objetivo**

Descrição do processo de mecanismos de *Business Continuity* aquando da migração de dados para o Datacenter *Disaster and Recovery* de Montijo, usando SRM.

2. **Âmbito**

Salvaguarda de toda a informação do Grupo Rangel.
Garantir a Disponibilidade da informação.

3. **Responsabilidades**

Técnicos de Suporte e Coordenador de Infraestruturas de IT.
Gestores de Projeto da Direção de Sistemas de Informação.

4. **Definições**

VM (Virtual Machine): sistema de computador virtual com o seu próprio CPU, memória, interface de rede e armazenamento, criado num sistema hardware físico, funcionando assim como "um computador dentro de um computador".

Cluster: arquitetura de um sistema capaz combinar vários computadores para trabalharem em conjunto ou pode denominar o grupo em si de computadores combinados.

SRM (Site Recovery Manager): é um sistema *"Disaster Recovery (DR)"* que fornece uma orquestração automatizada de *failover* e *failback* de forma a minimizar o tempo do processo de sincronização de recuperação de dados entre os *Datacenters*, primário e *backup*.

Array Pair: sendo um array um conjunto de elementos distintos, normalmente do mesmo tipo de dados agrupados numa estrutura, o seu pair será o conjunto storage ou em Alfena ou no Montijo.

Datastore (ou Datastore Group): é um repositório para armazenar, gerir e distribuir coleções de dados a um nível empresarial., podendo incorporar todos os tipos de dados que são produzidos, armazenados e usadas pela organização. Um *datastore group* pode conter mais que um *Datastore* que o SRM irá utilizar.

Protetion Group: grupo de *Virtual Machines* que serão recuperados em conjunto pelo SRM. Esses VMs contidos no *Protection Group*, possuem dados que foram replicados ou por *Aray-based replication* ou *vSphere replication*, não permitindo o *Protection Group* conter VMs replicados por mais de uma forma. Na Rangel, o SRM faz apenas replicação via *Array-base replication*.

Recovery Plan: contém todos os passos necessários para correr testes e migrações planeadas. Pode conter múltiplos *Protection Groups* podendo também incluir *Array-based replication* ou *Sphere Replication protection groups*.

5. **Modo de Proceder**

As organizações, de forma a operarem de forma eficiente e sem falhas, devem-se presenciar de um plano capaz de suportar a **continuidade de negócio** e operar as funções críticas de negócio durante eventos de emergência, como por exemplo, desastres naturais, crises comerciais, pandemias, violência no espaço de trabalho, ou qualquer outro evento que provoque disrupção das operações negociais.

O ***Plano de Disaster Recovery do Datacenter*** faz parte do plano de **Continuidade de Negócio**, responsável por manter a informação facilmente acessível após um evento de desastre ou incidente grave de cibersegurança, que coloque em causa a disponibilidade e integridade da informação. Assim sendo, é uma operação reativa, uma vez que consiste num conjunto de passos de maneira a permitir a retoma das atividades após esse desastre.

A Infraestrutura de Tecnologias da Informação da Rangel é composta pelos seguintes ambientes:

Tipo de Máquina	Quantidade	Localização	Horário de funcionamento	Indisponibilidade
[redacted]	2	[redacted]	Alinhado com as operações	[redacted]
[redacted]	2			
[redacted]	1			
[redacted]	2			

Atualmente, a solução implementada é baseada em *Datastore Groups* (*Array-based replication*).
Uma replicação é efetuada entre as duas *Storage Nimble* e a orquestração de *failover-failback* é feita pela *Appliance* SRM.

Elaborado: Luís Correia **Data: 20/04/2021** **Aprovado: Miguel Cordeiro** **Data: 27/04/2021**

Entrada em vigor: **27/04/2021**

DGSI.MOD.001/0

Figura 55 - Instrução de trabalho - Disaster Recovery do Datacentre

A instrução de trabalho "Gestão de Backups de Dados" está representada na Figura 56 e Figura 57.

Rangel

INSTRUÇÃO DE TRABALHO — **DSI.IT.011/3**

Gestão de Backups de Dados — **Página: 1 de 2**

1. **Objetivo**

Descrever as regras de funcionamento do registo e backups da informação dos servidores, bem como a replicação de toda a informação para o site de Disaster Recovery.

2. **Âmbito**

Salvaguarda de toda a informação do Grupo Rangel.

3. **Responsabilidades**

Técnicos de Suporte e Coordenador de Infraestruturas de IT.

4. **Definições**

Máquinas Low: Servidores de baixa criticidade para o negócio (ex: ambientes de teste ou de desenvolvimento).
Máquinas Medium: Servidores de média criticidade para o negócio (ex: máquinas que não armazenam dados, apenas aplicações).
Máquinas High: Servidores de elevada criticidade para o negócio (ex: máquinas que possuem dados operacionais).

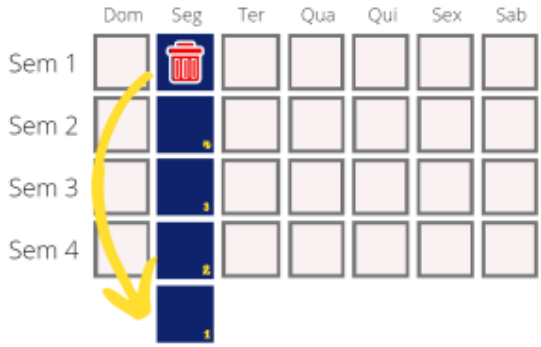
5. **Modo de Proceder**

O *Backup* aos PCs é realizado mediante cópia dos ficheiros fundamentais relacionados com a atividade de negócio do Grupo, para pasta partilhada no servidor alfdfs01, cabendo ao Colaborador a identificação desses mesmos ficheiros e a sua colocação na pasta partilhada. Devem também complementar a camada de proteção, com a utilização do OneDrive, e ativar o mecanismo de cópias de segurança das pastas principais: **Ambiente de Trabalho, Documentos e Imagens**.

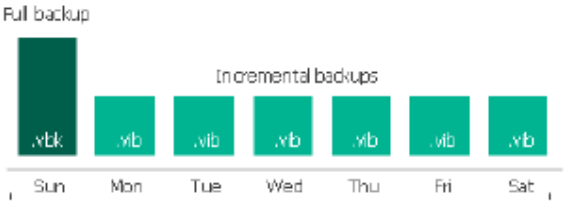
Os *Backups* a servidores e bases de dados são feitos de forma automática, sem intervenção de nenhum elemento da DSI. A monitorização à correta transferência de dados é realizada com recurso a um cockpit de gestão, através da ferramenta Veeam, que em caso de erro envia mensagem de alerta para a Equipa DSI – Infraestruturas. A salvaguarda dos dados é feita conforme descrito mais abaixo.

Máquinas Low:
Feito *full backup* semanal (por defeito à [redacted]) para um equipamento Storeonce localizado no Data Center em [redacted]
São retidos os últimos 4 *restore points*.

Os *restore poins* na cadeia de *backup* não são guardados sempre, eles são removidos de acordo com a política de retenção da organização. Aqui, foram definidos 4 *restore points*, para serem retidos no repositório do *backup*. Em cada semana, o *backup* adiciona, no repositório, a informação da semana atual. Ao reter 4 *restore points*, possuímos 4 "pastas", de modo a permitir a restauração da informação em 4 momentos diferentes no tempo. Na cópia número 5, o repositório apaga a informação da "pasta" mais antiga (no exemplo da imagem, "Semana 1"), de modo aguardar a informação da semana atual.



Máquinas Medium:
Feito *backup* incremental diário (por defeito às [redacted]) para um equipamento *Storeonce* localizado no *Data Center* em [redacted]
Semanalmente é feito um *full backup* (por defeito aos Domingos, às 00H00) para um equipamento *Storeonce* localizado no *Data Center* em [redacted]. São retidos os últimos 29 *restore points*.



Nesta situação, uma vez que a Rangel retém 29 *restore points*, isso permite a recuperação da informação até um máximo de 29 dias.

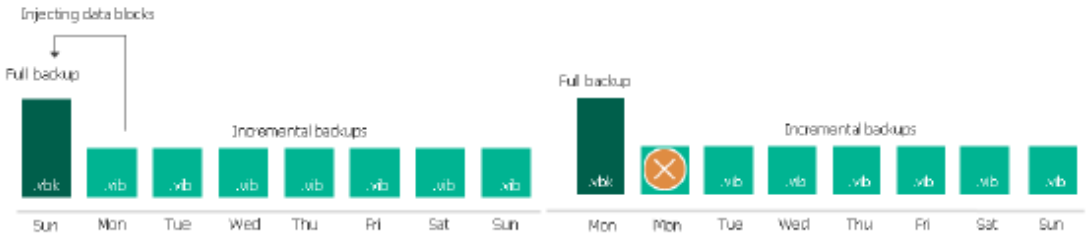
Na criação da cópia incremental número 30, o número permitido de *restore points* é excedido e há a transformação do processo. A primeira cópia *full backup* funde a informação com a cópia incremental seguinte, movendo assim a cópia *full backup* um dia, eliminando assim a cópia incremental desse dia. Este processo mantém-se sucessivamente até chegar à cópia *full backup* da semana seguinte.

Elaborado: Luís Correia — **Data: 20/04/2021** — **Aprovado: Miguel Cordeiro** — **Data: 27/04/2021**

Entrada em vigor: **27/04/2021**

DGSI.MOD.001/0

Figura 56 - Instrução de trabalho - Gestão de Backups de Dados (página 1/2)



Máquinas High:
Feito *backup* incremental de 6 em 6 horas para um equipamento NetApp localizado no Data Center em [redacted]. Semanalmente é feito um *full backup* (por defeito aos [redacted], às [redacted]) para um equipamento NetApp localizado no Data Center em [redacted]. São retidos os últimos 44 *restore points*.

Nesta situação, a janela de recuperação da informação é mais curta, apesar de um número maior de *restore points* (44), uma vez que a realização de cópias de seguranças é mais frequente, ou seja, com intervalos de tempo menores entre eles (6h entre cada *backup* incremental). Assim, podemos recuperar a informação até um máximo de 11 dias.

Replicação entre o Data Center Principal (Alfena) e o Data Center Disaster Recovery (Montijo)
Além do método de *backup* recorrendo à ferramenta Veeam, é realizada paralelamente, uma replicação a cada 5 minutos de toda a informação entre as duas *appliances* de *storage* (*HPE NIMBLE*), entre Data center de Alfena e o o Data Center de Disaster and Recovery, localizado na plataforma de [redacted].

Este mecanismo permite ao Grupo Rangel garantir um RPO (*Restore Point Objective*) até 5 minutos, e uma grande flexibilidade nas opções de restauro da informação de forma rápida, em caso de desastre, ou incidente grave de cibersegurança, que coloque em causa a disponibilidade e integridade da informação. Neste sentido, são retidos do lado do Data Center de Alfena 16 horas de *Restore Points*, enquanto que do lado do Montijo, são retidos 24 horas de *Restore Points*.

Quanto o tempo de *Restore Points* é excedido, o mesmo processo de transformação que acontece na ferramenta Veaam, também se aplica na replicação HPE NIMBLE.

Figura 57 - Instrução de trabalho - Gestão de Backups de Dados (página 2/2)

ANEXO 1 – OBJETIVOS DE CONTROLO E CONTROLOS DA ISO/IEC 27001:2013

Anexo A

(normativo)

Objetivos de controlo e controlos de referência

Os objetivos de controlo e controlos listados no Quadro A.1 são derivados diretamente de e são alinhados com os listados na ISO/IEC 27002:2013 secções 5 a 18 e devem ser usados no contexto da secção 6.1.3.

Quadro A.1 – Objetivos de Controlo e Controlos

A.5 Políticas de segurança da informação		
A.5.1 Diretrizes da gestão para a segurança da informação Objetivo: Proporcionar diretrizes e apoio da gestão para a segurança da informação, de acordo com os requisitos de negócio, leis e regulamentações relevantes.		
A.5.1.1	Políticas para a segurança da informação	*Controlo* Um conjunto de políticas para a segurança da informação deve ser definido, aprovado pela gestão, publicado e comunicado aos colaboradores e partes externas relevantes.
A.5.1.2	Revisão das políticas para a segurança da informação	*Controlo* As políticas para a segurança da informação devem ser revistas em intervalos planeados ou quando ocorrerem alterações significativas, de modo a assegurar a sua contínua aplicabilidade, adequabilidade e eficácia.
A.6 Organização de segurança da informação		
A.6.1 Organização interna Objetivo: Estabelecer um modelo de referência de gestão para iniciar e controlar a implementação e operação de segurança da informação dentro da organização.		
A.6.1.1	Papéis e responsabilidades de segurança da informação	*Controlo* Todas as responsabilidades de segurança da informação devem ser definidas e alocadas.
A.6.1.2	Segregação de funções	*Controlo* As funções e áreas de responsabilidades conflituantes devem ser segregadas para reduzir oportunidades para a modificação não autorizada ou não intencional, ou a utilização indevida dos ativos da organização.
A.6.1.3	Contacto com autoridades competentes	*Controlo* Devem ser mantidos contactos apropriados com as autoridades competentes que sejam relevantes.
A.6.1.4	Contacto com grupos de interesse especial	*Controlo* Devem ser mantidos contactos apropriados com grupos de interesse especial ou outros fóruns de especialistas de segurança e associações de profissionais.

(continua)

Figura 59 - Anexo A - ISO 27001:2013 (página 16/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.6.1.5	Segurança da informação na gestão de projeto	*Controlo* A segurança da informação deve ser endereçada na gestão de projeto, independentemente do tipo de projeto.
A.6.2 Dispositivos móveis e teletrabalho Objetivo: Assegurar a segurança no teletrabalho e na utilização de dispositivos móveis.		
A.6.2.1	Política de dispositivos móveis	*Controlo* Deve ser adotada uma política e as respetivas medidas de segurança para gerir os riscos introduzidos pela utilização de dispositivos móveis.
A.6.2.2	Teletrabalho	*Controlo* Deve ser implementada uma política e as respetivas medidas de segurança para proteger a informação acedida, processada ou armazenada em locais de teletrabalho.
A.7 Segurança na gestão de recursos humanos		
A.7.1 Antes da relação contratual Objetivo: Assegurar que os colaboradores e prestadores de serviço compreendem as suas responsabilidades, e que são adequados para as funções para as quais estão a ser considerados.		
A.7.1.1	Verificação de credenciais e referências	*Controlo* Devem ser realizadas verificações de credenciais e referências de todos os candidatos a uma relação contratual, de acordo com as leis, regulamentações e códigos de ética relevantes, e de forma proporcional aos requisitos de negócio, à classificação da informação que será acedida e aos riscos percecionados.
A.7.1.2	Termos e condições da relação contratual	*Controlo* Os acordos contratuais com os colaboradores e prestadores de serviço devem estabelecer as suas responsabilidades e as da organização relativamente à segurança da informação.
A.7.2 Durante a relação contratual Objetivo: Assegurar que os colaboradores e prestadores de serviço estão conscientes e cumprem as suas responsabilidades de segurança da informação.		
A.7.2.1	Responsabilidades da gestão	*Controlo* A gestão deve requerer a todos os colaboradores e prestadores de serviço que apliquem a segurança da informação, de acordo com os procedimentos e políticas estabelecidos pela organização.
A.7.2.2	Consciencialização, educação e formação em segurança da informação	*Controlo* Todos os colaboradores da organização e, quando relevante, os prestadores de serviço devem ser destinatários de ações de consciencialização, educação e formação apropriadas, bem como de atualizações regulares nas políticas e procedimentos da organização que sejam relevantes para o desempenho da sua função.
A.7.2.3	Procedimento disciplinar	*Controlo* Deve existir e ser comunicado um procedimento disciplinar formal que seja acionável em relação aos colaboradores que tenham cometido uma violação de segurança da informação.

(continua)

Figura 58 - Anexo A - ISO 27001:2013 (página 17/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.7.3 Cessação e alteração da relação contratual Objetivo: Proteger os interesses da organização no processo de cessação ou alteração da relação contratual.		
A.7.3.1	Responsabilidades na cessação ou alteração da relação contratual	*Controlo* Devem ser definidas, comunicadas e asseguradas as responsabilidades e deveres de segurança da informação que permaneçam válidas após a cessação ou alteração da relação contratual com os colaboradores ou prestadores de serviço.
A.8 Gestão de ativos		
A.8.1 Responsabilidade pelos ativos Objetivo: Identificar os ativos da organização e definir responsabilidades de proteção apropriadas.		
A.8.1.1	Inventário de ativos	*Controlo* Devem ser identificados os ativos associados com a informação e os recursos de processamento de informação e deve ser criado e mantido um inventário destes ativos.
A.8.1.2	Responsabilidade pelos ativos	*Controlo* Os ativos registados no inventário devem ter um responsável.
A.8.1.3	Utilização aceitável de ativos	*Controlo* Devem ser identificadas, documentadas e implementadas regras para a utilização aceitável da informação, dos ativos associados com a informação e dos recursos de processamento de informação.
A.8.1.4	Devolução de ativos	*Controlo* Todos os colaboradores e utilizadores de entidades externas devem devolver os ativos da organização que estejam na sua posse no momento da cessação da relação contratual ou acordo.
A.8.2 Classificação da informação Objetivo: Assegurar que a informação recebe um nível adequado de proteção, de acordo com a sua importância para a organização.		
A.8.2.1	Classificação da informação	*Controlo* A informação deve ser classificada com base nos requisitos legais, valor, importância e sensibilidade em caso de divulgação ou modificação não autorizada.
A.8.2.2	Etiquetagem da informação	*Controlo* Deve ser desenvolvido e implementado um conjunto de procedimentos apropriados para a etiquetagem da informação, de acordo com o esquema de classificação da informação adotado pela organização.
A.8.2.3	Manuseamento de ativos	*Controlo* Devem ser desenvolvidos e implementados procedimentos para o manuseamento de ativos, de acordo com o esquema de classificação da informação adotado pela organização.
A.8.3 Manuseamento de suportes de dados Objetivo: Prevenir a divulgação não autorizada, modificação, remoção ou eliminação da informação armazenada em suportes de dados.		

Figura 61 - Anexo A - ISO 27001:2013 (página 18/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.8.3.1	Gestão de suportes de dados amovíveis	*Controlo* Devem ser implementados procedimentos para a gestão de suportes de dados amovíveis, de acordo com o esquema de classificação adotado pela organização.
A.8.3.2	Eliminação de suportes de dados	*Controlo* Os suportes de dados devem ser eliminados de forma segura, quando deixarem de ser necessários, através da utilização de procedimentos formais.
A.8.3.3	Transporte de suportes de dados	*Controlo* Os suportes de dados devem ser protegidos contra acessos não autorizados, utilização indevida ou corrupção durante o seu transporte.
A.9 Controlo de acesso		
A.9.1 Requisitos de negócio para controlo de acesso Objetivo: Limitar o acesso à informação e aos recursos de processamento de informação.		
A.9.1.1	Política de controlo de acesso	*Controlo* Deve ser estabelecida, documentada e revista uma política de controlo de acesso, tendo como base os requisitos de negócio e de segurança da informação.
A.9.1.2	Acesso a redes e a serviços de rede	*Controlo* Aos utilizadores apenas deve ser atribuído acesso à rede e a serviços de rede para os quais tenham sido especificamente autorizados a utilizar.
A.9.2 Gestão de acesso de utilizadores Objetivo: Assegurar o acesso de utilizadores autorizados e prevenir o acesso não autorizado a sistemas e serviços.		
A.9.2.1	Registo e cancelamento de utilizador	*Controlo* Deve ser implementado um processo formal de registo e cancelamento de utilizadores para assegurar a atribuição de direitos de acesso.
A.9.2.2	Disponibilização de acesso aos utilizadores	*Controlo* Deve ser implementado um processo formal de disponibilização de acesso aos utilizadores para atribuir ou revogar os direitos de acesso para todos os tipos de utilizadores em todos os sistemas e serviços.
A.9.2.3	Gestão de direitos de acesso privilegiado	*Controlo* A atribuição e utilização de direitos de acesso privilegiado devem ser restritas e controladas.

(continua)

Figura 60 - Anexo A - ISO 27001:2013 (página 19/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.9.2.4	Gestão da informação secreta para autenticação de utilizadores	*Controlo* A atribuição da informação secreta para autenticação deve ser controlada através de um processo formal de gestão.
A.9.2.5	Revisão de direitos de acesso de utilizadores	*Controlo* Os responsáveis pelos ativos devem rever os direitos de acesso dos utilizadores em intervalos regulares.
A.9.2.6	Remoção ou ajuste de direitos de acesso	*Controlo* Os direitos de acesso à informação e aos recursos de processamento de informação, de todos os colaboradores e utilizadores de entidades externas, devem ser removidos após a cessação de relação contratual ou acordo, ou ajustados em caso de alteração destes.
A.9.3 Responsabilidades dos utilizadores Objetivo: Tornar os utilizadores responsáveis pela proteção da sua informação de autenticação.		
A.9.3.1	Utilização da informação secreta para autenticação	*Controlo* Deve ser exigido aos utilizadores o cumprimento das práticas da organização na utilização da informação secreta para autenticação.
A.9.4 Controlo de acesso a sistemas e aplicações Objetivo: Prevenir o acesso não autorizado a sistemas e aplicações.		
A.9.4.1	Restrição de acesso à informação	*Controlo* O acesso à informação e funções de sistema das aplicações deve ser limitado de acordo com a política de controlo de acesso.
A.9.4.2	Procedimentos seguros de início de sessão	*Controlo* Quando exigido pela política de controlo de acesso, o acesso a sistemas e aplicações deve ser controlado por um procedimento seguro de início de sessão.
A.9.4.3	Sistema de gestão de senhas	*Controlo* Os sistemas para gestão de senhas devem ser interativos e devem assegurar a qualidade da senha.
A.9.4.4	Utilização de programas utilitários privilegiados	*Controlo* A utilização de programas utilitários que se possam sobrepor aos controlos dos sistemas e aplicações deve ser restringida e controlada de forma rígida.
A.9.4.5	Controlo de acesso ao código fonte de programas	*Controlo* O acesso ao código fonte de programas deve ser restrito.

Figura 63 - Anexo A - ISO 27001:2013 (página 20/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.10 Criptografia		
A.10.1 Controlos criptográficos Objetivo: Assegurar a utilização adequada e eficaz de criptografia para proteger a confidencialidade, autenticidade e/ou integridade da informação.		
A.10.1.1	Política sobre a utilização de controlos criptográficos	*Controlo* Deve ser desenvolvida e implementada uma política sobre a utilização de controlos criptográficos para proteção da informação.
A.10.1.2	Gestão de chaves	*Controlo* Deve ser desenvolvida e implementada uma política sobre a utilização, proteção e vida útil das chaves criptográficas ao longo de todo o seu ciclo de vida.
A.11 Segurança física e ambiental		
A.11.1 Áreas seguras Objetivo: Prevenir o acesso físico não autorizado, os danos e as interferências na informação e nos recursos de processamento de informação da organização.		
A.11.1.1	Perímetro de segurança física	*Controlo* Devem ser definidos e utilizados perímetros de segurança para proteger as áreas que contenham informação sensível ou crítica e recursos de processamento de informação.
A.11.1.2	Controlos de entrada física	*Controlo* As áreas seguras devem ser protegidas através de controlos de entrada apropriados que assegurem que apenas é permitido o acesso a pessoas autorizadas.
A.11.1.3	Segurança em escritórios, salas e instalações	*Controlo* Devem ser concebidas e aplicadas medidas de segurança física para escritórios, salas e instalações.
A.11.1.4	Proteção contra ameaças externas e ambientais	*Controlo* Devem ser concebidas e aplicadas medidas de proteção física contra desastres naturais, ataques maliciosos ou acidentes.
A.11.1.5	Trabalhar em áreas seguras	*Controlo* Devem ser concebidos e aplicados procedimentos para trabalhar em áreas seguras.
A.11.1.6	Áreas de carga e descarga	*Controlo* Os pontos de acesso, tais como as áreas de carga e descarga e outros pontos onde pessoas não autorizadas possam entrar nas instalações, devem ser controlados e, se possível, isolados dos recursos de processamento de informação para evitar o acesso não autorizado.
A.11.2 Equipamento Objetivo: Prevenir a perda, dano, furto ou comprometimento de ativos e interrupção das operações da organização.		
A.11.2.1	Colocação e proteção de equipamentos	*Controlo* Os equipamentos devem ser colocados e protegidos de forma a reduzir os riscos de ameaças e perigos ambientais, e as oportunidades para acesso não autorizado.

Figura 62 - Anexo A - ISO 27001:2013 (página 21/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.11.2.2	Serviços básicos de suporte	*Controlo* Os equipamentos devem ser protegidos contra interrupções de energia elétrica e outras falhas causadas pelos serviços básicos de suporte.
A.11.2.3	Segurança da cablagem	*Controlo* A cablagem elétrica e de telecomunicações que transporta dados ou que suporta os serviços de informação deve ser protegida contra interceção, interferência ou dano.
A.11.2.4	Manutenção de equipamentos	*Controlo* Os equipamentos devem ser mantidos de forma correta para assegurar a sua contínua disponibilidade e integridade.
A.11.2.5	Remoção de ativos	*Controlo* Os equipamentos, informação ou software não devem ser retirados das instalações sem autorização prévia.
A.11.2.6	Segurança de equipamentos e ativos fora das instalações	*Controlo* Devem ser aplicadas medidas de segurança aos ativos fora das instalações, tendo em consideração os diferentes riscos decorrentes do trabalho fora das instalações da organização.
A.11.2.7	Eliminação e reutilização seguras de equipamentos	*Controlo* Todos os itens de equipamentos contendo suporte de dados devem ser verificados antes da sua eliminação ou reutilização para assegurar que qualquer dado sensível e software licenciado é removido ou eliminado através de reescrita segura.
A.11.2.8	Equipamento de utilizador não vigiado	*Controlo* Os utilizadores devem assegurar que os equipamentos não vigiados têm uma proteção adequada.
A.11.2.9	Política de secretária limpa e ecrã limpo	*Controlo* Deve ser adotada uma política de secretária limpa de papéis e suportes de dados amovíveis e uma política de ecrã limpo para os recursos de processamento de informação.
A.12 Segurança de operações		
A.12.1 Procedimentos e responsabilidades operacionais Objetivo: Assegurar a operação correta e segura dos recursos de processamento de informação.		
A.12.1.1	Procedimentos de operação documentados	*Controlo* Os procedimentos de operação devem ser documentados e disponibilizados a todos os utilizadores que deles necessitem.
A.12.1.2	Gestão de alterações	*Controlo* As alterações na organização, processos de negócio, recursos de processamento de informação e nos sistemas que afetem a segurança da informação devem ser controladas.

Figura 64 - Anexo A - ISO 27001:2013 (página 22/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.12.1.3	Gestão da capacidade	*Controlo* A utilização dos recursos deve ser monitorizada e ajustada e devem ser elaboradas projeções para os requisitos de capacidade futura, de modo a assegurar o necessário desempenho dos sistemas.
A.12.1.4	Separação entre ambientes de desenvolvimento, teste e de produção	*Controlo* Os ambientes de desenvolvimento, teste e de produção devem ser separados para reduzir os riscos de acesso não autorizado ou alterações no ambiente de produção.
A.12.2 Proteção contra código malicioso Objetivo: Assegurar que a informação e os recursos de processamento de informação estão protegidos contra código malicioso.		
A.12.2.1	Controlos contra código malicioso	*Controlo* Devem ser implementados controlos de deteção, prevenção e recuperação para proteger contra código malicioso, em conjugação com ações apropriadas de consciencialização dos utilizadores.
A.12.3 Salvaguarda de dados Objetivo: Proteger contra a perda de dados.		
A.12.3.1	Salvaguarda de informação	*Controlo* Devem ser efetuadas e testadas, de forma regular, as cópias de salvaguarda de informação, softwares e imagens de sistemas, conforme a política de salvaguarda de informação.
A.12.4 Registos de eventos e monitorização Objetivo: Registar eventos e gerar evidências.		
A.12.4.1	Registos de eventos	*Controlo* Devem ser produzidos, mantidos e revistos de forma regular os registos de eventos que contenham informação sobre as atividades dos utilizadores, exceções, falhas e eventos de segurança da informação.
A.12.4.2	Proteção da informação registada	*Controlo* Os recursos de registo e as informações registadas devem ser protegidas contra a adulteração e acesso não autorizado.
A.12.4.3	Registos de administrador e de operador	*Controlo* As atividades dos administradores e dos operadores de sistema devem ser registadas e os registos ser protegidos e revistos regularmente.

Figura 65 - Anexo A - ISO 27001:2013 (página 23/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.12.4.4	Sincronização de relógio	*Controlo* Os relógios de todos os sistemas relevantes de processamento de informação numa organização ou num domínio de segurança devem ser sincronizados, de acordo com uma única referência horária.
A.12.5 Controlo de software em sistemas de produção Objetivo: Assegurar a integridade dos sistemas de produção.		
A.12.5.1	Instalação de software nos sistemas de produção	*Controlo* Devem ser implementados procedimentos para controlar a instalação de software nos sistemas de produção.
A.12.6 Gestão de vulnerabilidades técnicas Objetivo: Prevenir a exploração de vulnerabilidades técnicas.		
A.12.6.1	Gestão de vulnerabilidades técnicas	Controlo A informação sobre as vulnerabilidades técnicas dos sistemas de informação em utilização deve ser obtida de forma atempada, a exposição da organização a estas vulnerabilidades deve ser avaliada, e ser tomadas medidas apropriadas para endereçar os riscos associados.
A.12.6.2	Restrições sobre a instalação de software	*Controlo* Devem ser estabelecidas e implementadas regras sobre a instalação de software pelos utilizadores.
A.12.7 Considerações para auditorias a sistemas de informação Objetivo: Minimizar o impacto das atividades de auditoria nos sistemas de produção.		
A.12.7.1	Controlos de auditoria nos sistemas de informação	*Controlo* Os requisitos e atividades de auditoria que envolvam verificações nos sistemas de produção devem ser planeados de forma cuidada e acordados para minimizar as interrupções nos processos de negócio.
A.13 Segurança de comunicações		
A.13.1 Gestão de segurança da rede Objetivo: Assegurar a proteção da informação nas redes e nos seus recursos de processamento de informação.		
A.13.1.1	Controlos da rede	*Controlo* As redes devem ser geridas e controladas para proteger a informação nos sistemas e nas aplicações.
A.13.1.2	Segurança de serviços de rede	*Controlo* Os mecanismos de segurança, níveis de serviço e requisitos de gestão para todos os serviços de rede devem ser identificados e incluídos nos acordos para serviços de rede, independentemente desses serviços prestados serem internos ou externos.

Figura 66 - Anexo A - ISO 27001:2013 (página 24/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.13.1.3	Segregação das redes	*Controlo* Os grupos de serviços de informação, utilizadores e sistemas de informação devem ser segregados em redes.
A.13.2 Transferência de informação Objetivo: Manter a segurança da informação transferida dentro da organização e para qualquer entidade externa.		
A.13.2.1	Políticas e procedimentos de transferência de informação	*Controlo* Devem existir políticas, procedimentos e controlos formais para proteger a transferência da informação através da utilização de qualquer tipo de meio de comunicação.
A.13.2.2	Acordos sobre transferência de informação	*Controlo* Os acordos devem endereçar a transferência segura de informação de negócio entre a organização e entidades externas.
A.13.2.3	Mensagens eletrónicas	Controlo A informação contida nas mensagens eletrónicas deve ser protegida de forma apropriada.
A.13.2.4	Acordos de confidencialidade ou de não divulgação	Controlo Devem ser identificados, revistos regularmente e documentados os requisitos para acordos de confidencialidade ou de não divulgação que reflitam as necessidades da organização para proteção da informação.
A.14 Aquisição, desenvolvimento e manutenção de sistemas		
A.14.1 Requisitos de segurança de sistemas de informação Objetivo: Assegurar que a segurança da informação é uma parte integrante dos sistemas de informações ao longo do todo o seu ciclo de vida. Isto inclui também os requisitos para sistemas de informação que prestam serviços através de redes públicas.		
A.14.1.1	Especificação e análise de requisitos de segurança da informação	*Controlo* Os requisitos relacionados com a segurança da informação devem ser incluídos nos requisitos para novos sistemas de informação ou para melhorias nos sistemas de informação existentes.
A.14.1.2	Proteger serviços aplicacionais nas redes públicas	*Controlo* A informação envolvida em serviços aplicacionais transmitida nas redes públicas deve ser protegida contra atividades fraudulentas, disputas contratuais e divulgação e modificação não autorizadas.
A.14.1.3	Proteger transações de serviços aplicacionais	*Controlo* A informação envolvida nas transações de serviços aplicacionais deve ser protegida para prevenir a transmissão incompleta, encaminhamento incorreto, alteração não autorizada, divulgação não autorizada, duplicação ou repetição não autorizada da mensagem.
A.14.2 Segurança no desenvolvimento e nos processos de suporte Objetivo: Assegurar que a segurança da informação é concebida e implementada no âmbito do ciclo de vida do desenvolvimento de sistemas de informação.		
A.14.2.1	Política de desenvolvimento seguro	*Controlo* Devem ser estabelecidas regras para o desenvolvimento de software e de sistemas e aplicadas ao desenvolvimento realizado na organização.

Figura 67 - Anexo A - ISO 27001:2013 (página 25/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.14.2.2	Procedimentos de controlo de alterações aos sistemas	*Controlo* As alterações aos sistemas no ciclo de vida do desenvolvimento devem ser controladas através da utilização de procedimentos formais de controlo de alterações.
A.14.2.3	Revisão técnica de aplicações após alterações na plataforma de produção	*Controlo* Quando as plataformas de produção são alteradas, as aplicações críticas de negócios devem ser revistas e testadas para assegurar que não há nenhum impacto adverso sobre as operações ou segurança da organização.
A.14.2.4	Restrições sobre alterações em pacotes de software	*Controlo* As alterações nos pacotes de software devem ser desencorajadas, limitadas às mudanças necessárias e todas as alterações devem ser estritamente controladas.
A.14.2.5	Princípios de engenharia de sistemas seguros	*Controlo* Devem ser estabelecidos, documentados, mantidos e aplicados princípios de engenharia de sistemas seguros para todas as iniciativas de implementação de sistemas de informação.
A.14.2.6	Ambiente de desenvolvimento seguro	*Controlo* As organizações devem estabelecer e proteger, de forma apropriada, ambientes de desenvolvimento seguro para as iniciativas de desenvolvimento e integração de sistemas, que abranjam todo o ciclo de vida do desenvolvimento de sistemas.
A.14.2.7	Desenvolvimento subcontratado	*Controlo* A organização deve supervisionar e monitorizar a atividade subcontratada de desenvolvimento de sistemas.
A.14.2.8	Testes de segurança de sistemas	*Controlo* Devem ser realizados testes das funcionalidades de segurança durante o desenvolvimento.
A.14.2.9	Testes de aceitação de sistemas	*Controlo* Devem ser estabelecidos programas de testes de aceitação e respetivos critérios de aceitação para novos sistemas de informação, atualizações e novas versões.
A.14.3 Dados de teste Objetivo: Assegurar a proteção dos dados usados para testes.		
A.14.3.1	Proteção de dados de teste	*Controlo* Os dados de teste devem ser selecionados cuidadosamente, protegidos e controlados.
A.15 Relações com fornecedores		
A.15.1 Segurança da informação nas relações com os fornecedores Objetivo: Assegurar a proteção dos ativos da organização que estão acessíveis aos fornecedores.		
A.15.1.1	Política de segurança da informação para as relações com fornecedores	*Controlo* Os requisitos de segurança da informação para a mitigação dos riscos associados ao acesso de fornecedores aos ativos da organização devem ser acordados com os fornecedores e documentados.

Figura 69 - Anexo A - ISO 27001:2013 (página 26/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.15.1.2	Endereçar a segurança nos acordos com os fornecedores	*Controlo* Todos os requisitos de segurança da informação relevantes devem ser estabelecidos e acordados com cada fornecedor que possa aceder, processar, armazenar, comunicar ou fornecer componentes de infraestrutura de TI para a informação da organização.
A.15.1.3	Cadeia de fornecimento de tecnologias de informação e comunicação	*Controlo* Os acordos com fornecedores devem incluir requisitos para endereçar os riscos de segurança da informação associados aos serviços de tecnologias da informação e comunicação e à cadeia de fornecimento de produtos.
A.15.2 Gestão da entrega de serviços pelos fornecedores Objetivo: Manter o nível acordado de segurança da informação e de disponibilização de serviços, alinhado com os acordos com fornecedores.		
A.15.2.1	Monitorizar e rever serviços de fornecedores	*Controlo* As organizações devem, de forma regular, monitorizar, rever e auditar a disponibilização de serviços pelos fornecedores.
A.15.2.2	Gerir alterações aos serviços de fornecedores	*Controlo* As alterações ao fornecimento dos serviços pelos fornecedores, incluindo a manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controlos existentes, devem ser geridas, tendo em consideração a criticidade da informação, dos sistemas e dos processos de negócio envolvidos e a reavaliação dos riscos.
A.16 Gestão de incidentes de segurança da informação		
A.16.1 Gestão de incidentes de segurança da informação e melhorias Objetivo: Assegurar uma abordagem consistente e eficaz à gestão de incidentes de segurança da informação, incluindo a comunicação de eventos e pontos fracos de segurança.		
A.16.1.1	Responsabilidades e procedimentos	*Controlo* Devem ser estabelecidos procedimentos e responsabilidades de gestão para assegurar uma resposta célere, eficaz e ordenada aos incidentes de segurança da informação.
A.16.1.2	Reportar eventos de segurança da informação	*Controlo* Os eventos de segurança da informação devem ser reportados através dos canais de gestão apropriados, o mais rapidamente possível.
A.16.1.3	Reportar pontos fracos de segurança da informação	*Controlo* Os colaboradores e os prestadores de serviço que utilizam os serviços e os sistemas de informação da organização devem ser instruídos a detetar e reportar qualquer ponto fraco de segurança da informação, observado ou suspeito, nos sistemas ou serviços.
A.16.1.4	Avaliação e decisão sobre eventos de segurança da informação	*Controlo* Os eventos de segurança da informação devem ser avaliados e deve ser decidido se os mesmos serão classificados como incidentes de segurança da informação.
A.16.1.5	Resposta a incidentes de segurança da informação	*Controlo* Os incidentes de segurança da informação devem ser respondidos de acordo com os procedimentos documentados.

Figura 68 - Anexo A - ISO 27001:2013 (página 27/32)

Quadro A.1 – Objetivos de Controlo e Controlos (continuação)

A.16.1.6	Aprender com os incidentes de segurança da informação	*Controlo* O conhecimento obtido através da análise e resolução de incidentes de segurança da informação deve ser empregue de forma a reduzir a probabilidade ou o impacto de futuros incidentes.
A.16.1.7	Recolha de evidências	*Controlo* A organização deve definir e aplicar procedimentos para a identificação, recolha, obtenção e preservação da informação, que possa servir como evidência.
A.17 Aspetos de segurança da informação na gestão da continuidade do negócio		
A.17.1 Continuidade de segurança da informação Objetivo: A continuidade de segurança da informação deve ser contemplada nos sistemas de gestão da continuidade do negócio da organização.		
A.17.1.1	Planeamento da continuidade de segurança da informação	*Controlo* A organização deve determinar os seus requisitos de segurança da informação e a continuidade da gestão de segurança da informação em situações adversas, por exemplo durante uma crise ou um desastre.
A.17.1.2	Implementação da continuidade de segurança da informação	*Controlo* A organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controlos para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa.
A.17.1.3	Verificar, rever e avaliar a continuidade de segurança da informação	*Controlo* A organização deve verificar os controlos de continuidade de segurança da informação estabelecidos e implementados em intervalos regulares, para assegurar que estes são válidos e eficazes em situações adversas.
A.17.2 Redundâncias Objetivo: Assegurar a disponibilidade dos recursos de processamento da informação.		
A.17.2.1	Disponibilidade dos recursos de processamento da informação	*Controlo* Os recursos de processamento da informação devem ser implementados com a redundância necessária para cumprir os requisitos de disponibilidade.
A.18 Conformidade		
A.18.1 Conformidade com requisitos legais e contratuais Objetivo: Evitar violações de obrigações legais, estatutárias, regulamentares ou contratuais relacionadas com a segurança da informação e de quaisquer requisitos de segurança.		
A.18.1.1	Identificação da legislação aplicável e de requisitos contratuais	*Controlo* Todos os requisitos legais, estatutários, regulamentares, contratuais relevantes bem como a abordagem da organização para cumprir esses requisitos devem ser identificados explicitamente, documentados e mantidos atualizados, para cada sistema de informação e para a organização.

Figura 71 - Anexo A - ISO 27001:2013 (página 28/32)

Quadro A.1 – Objetivos de Controlo e Controlos (conclusão)

A.18.1.2	Direitos de propriedade intelectual	*Controlo* Devem ser implementados procedimentos apropriados para assegurar a conformidade com os requisitos legais, regulamentares e contratuais relativos aos direitos de propriedade intelectual e à utilização de produtos de software proprietário.
A.18.1.3	Proteção de registos	*Controlo* Os registos devem ser protegidos contra a perda, eliminação, falsificação, acesso não autorizado e divulgação não autorizada, de acordo com os requisitos legais, regulamentares, contratuais e de negócio.
A.18.1.4	Privacidade e proteção de dados pessoais	*Controlo* A privacidade e a proteção de dados pessoais devem ser asseguradas conforme estabelecido pela legislação e regulamentação relevante, onde aplicável.
A.18.1.5	Regulamentação de controlos criptográficos	*Controlo* Os controlos criptográficos devem ser utilizados em conformidade com todos os acordos, leis e regulamentos relevantes.
A.18.2 Revisões de segurança da informação Objetivo: Assegurar que a segurança da informação é implementada e operada de acordo com as políticas e procedimentos organizacionais.		
A.18.2.1	Revisão independente de segurança da informação	*Controlo* A abordagem da organização para gerir a segurança da informação e a sua implementação (ou seja, objetivos de controlo, controlos, políticas, processos e procedimentos de segurança da informação) devem ser revistos de forma independente, em intervalos planeados ou quando ocorrerem alterações significativas.
A.18.2.2	Conformidade com as políticas e normas de segurança	*Controlo* Os gestores devem rever regularmente a conformidade do processamento da informação e dos procedimentos dentro da sua área de responsabilidade com as políticas de segurança, normas e quaisquer outros requisitos de segurança apropriados.
A.18.2.3	Revisão da conformidade técnica	*Controlo* Os sistemas de informação devem ser revistos regularmente quanto à sua conformidade com as políticas e normas de segurança da informação da organização.

Figura 70 - Anexo A - ISO 27001:2013 (página 29/32)

ANEXO 2 – NORMAS QUE PERTENCEM À FAMÍLIA DE NORMAS DA ISO 27000

ISO-Norm	Title	Status
ISO 27000	Information security management systems—Overview and vocabulary	published 2009
ISO 27001	Information security management systems—Requirements	published 2005
ISO 27002	Code of practice for information security management	published 2007
ISO 27003	Information security management system implementation guidance	published 2010
ISO 27004	Information security management—Measurement	published 2009
ISO 27005	Information security risk management	published 2011
ISO 27006	Requirements for bodies providing audit and certification of ISMSs	published 2011
ISO 27007	Guidelines for ISMS auditing	published 2011
ISO 27008	Guidelines for auditors on ISMS controls	published 2011
ISO 27010	ISMSs for inter-sector and inter-organizational communications	published 2012
ISO 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	published 2008
ISO 27013	Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001	under development
ISO 27014	Proposal on an information security governance (ISG) framework	under development
ISO 27016	Information security management—Organizational economics	under development
ISO 27017	Guidelines on information security controls for use of cloud computing	under development
ISO 27018	Code of practice for data protection controls for public cloud computing	under development
ISO 27031	Guidelines for ICT readiness for business continuity	under development
ISO 27032	Guidelines for cyber security	under development
ISO 27033-1	Network security—Part 1: Overview and concepts	published 2009
ISO 27033-2	Network security—Part 2: Guidelines for the design and implementation	published 2012
ISO 27033-3	Network security—Part 3: Reference networking scenarios	published 2010
ISO 27033-4	Network security—Part 4: Securing communications between networks	under development
ISO 27033-5	Network security—Part 5: Securing communications across networks using VPNs	under development
ISO 27033-6	Network security—Part 6: Securing IP network access using wireless	under development
ISO 27034-1	Application security—Part 1: Overview and concepts	published 2011
ISO 27034-2	Application security—Part 2: Organization normative framework	under development
ISO 27034-3	Application security—Part 3: Application security management process	under development
ISO 27034-4	Application security—Part 4: Application security validation	under development
ISO 27034-5	Application security—Part 5: Application security controls data structure	under development
ISO 27035	Information security incident management	under development
ISO 27036	Information security for supplier relationships	under development
ISO 27037	Guidelines for identification, collection and/or acquisition and preservation of digital evidence	under development
ISO 27038	Specification for digital redaction	under development
ISO 27039	Selection, deployment and operations of intrusion detection systems	under development
ISO 27040	Storage security	under development
ISO 27041	Guidance on assuring suitability and adequacy of investigation methods	under development
ISO 27042	Guidelines for the analysis and interpretation of digital evidence	under development
ISO 27043	Investigation principles and processes	under development

Figura 72 - Família de normas da ISO 27000