Instituto Politécnico de Tomar

Escola Superior de Gestão de Tomar

Avaliação da Segurança de Sistemas de Informação nas Autarquias Locais: Um Estudo de Caso no Município de Torres Novas

Projeto

Ana Sofia Cassis dos Santos

Mestrado em Auditoria e Finanças

Tomar . junho . 2021

Instituto Politécnico de Tomar

Escola Superior de Gestão

Avaliação da Segurança de Sistemas de Informação nas Autarquias Locais: Um Estudo de Caso no Município de Torres Novas

Projeto

Ana Sofia Cassis dos Santos

Orientado por:
Especialista Carlos Fernando Calhau Trigacheiro – Instituto Politécnico de Tomar
Doutor Célio Gonçalo Cardoso Marques – Instituto Politécnico de Tomar

Projeto apresentada ao Instituto Politécnico de Tomar para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria e Finanças

Dedico este trabalho aos meus filhos, Martim e Leonor

AGRADECIMENTOS

A realização do presente projeto de mestrado é o culminar de uma importante etapa da minha vida, envolveu um enorme esforço e dedicação pessoal e contou com apoios e incentivos decisivos, pelos quais desejo exprimir o meu sincero reconhecimento.

À minha família, em especial ao meu marido e filhos, pela sólida presença e apoio incondicional, que apesar de se verem privados da minha companhia em virtude da realização deste trabalho se mantiveram sempre ao meu lado, incentivando-me e apoiando-me para atingir os meus objetivos.

Aos meus orientadores Doutor Célio Marques e Dr. Carlos Trigacheiro, pela disponibilidade manifestada desde o primeiro momento, rigor científico, revisão crítica, apoio e orientação ao longo deste percurso.

Ao Município de Torres Novas, na pessoa do seu presidente Dr. Pedro Ferreira pela aprovação da realização deste trabalho, à Dra. Isabel Ribeiro principal impulsionadora deste projeto e à Divisão de Informática, pela disponibilidade, apoio e por me proporcionarem as condições para a concretização deste projeto.

Aos amigos, pelo apoio, força, alegria e ânimo que me transmitiram ao longo deste percurso.

Aos colegas de mestrado que comigo trilharam este caminho, pelo apoio prestado durantes estes dois anos e que me enriqueceram tanto a nível académico como pessoal.

A todos vós,

Muito Obrigada!

RESUMO

Numa Era caracterizada pela importância da informação, a generalidade das organizações depende fortemente dos Sistemas de Informação para o desempenho da sua missão.

Para as Autarquias Locais, onde se verificam constantes mudanças nos processos organizacionais com o objetivo de uma melhor utilização económica, eficiente e equitativa dos recursos públicos, os Sistemas de Informação são um fator-chave. Ao lidarem diariamente com informação confidencial estão sujeitas a obrigações de conformidade ética e legal que geram grande responsabilidade na gestão da informação que tratam e produzem.

A par com a evolução das tecnologias de informação e da dependência crescente entre bom funcionamento das instituições e o normal funcionamento dos Sistemas de Informação está o aumento da criminalidade informática que se manifesta através de técnicas de intrusão e aproveitamento de vulnerabilidades, o que impõe melhorias aos paradigmas da segurança.

Por sua vez, a Segurança da Informação trata da proteção dos Sistemas de Informação impedindo o acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados da informação, de forma a preservar a confidencialidade, integridade/autenticidade e disponibilidade da mesma.

De facto, no domínio da investigação observa-se a existência de um número razoável de estudos sobre Segurança de Sistemas de Informação e sobre a aplicação da ISO/IEC 27002:2013, contudo, o número de estudos aplicados a Autarquias Locais em Portugal é praticamente inexistente, com este trabalho visa contribuir-se para colmatar esta lacuna.

Com este estudo de caso pretendeu-se aferir, através da aplicação de um inquérito por questionário baseado na ISO/IEC 27002:2013 associado a um modelo de maturidade qual o grau de maturidade dos controlos de segurança do Sistema de Informação no Município de Torres Novas.

A aplicação destas duas ferramentas em conjunto permitiu medir o nível de maturidade dos controlos se segurança do Sistema de Informação do Município e identificar de forma quantitativa quais as áreas mais críticas.

Palavras-chave: Autarquias Locais, ISO/IEC 27002:2013, modelo de maturidade, Segurança da Informação

ABSTRACT

In an Era characterized by the importance of information, most organizations depend heavily on information systems to perform their mission.

For Local Governments, where there are constant changes in organizational processes with the aim of better economic, efficient and equitable use of public resources, information systems are a key factor. When dealing daily with confidential information they are subject to ethical and legal compliance obligations that generate great responsibility in the management of the information they treat and produce.

Along with the evolution of information technologies and the growing dependence between the good functioning of institutions and the normal functioning of information systems is the increase in computer crime, which manifests itself through intrusion techniques and the exploitation of vulnerabilities, which imposes improvements to security paradigms.

In turn, information security is about protecting information systems by preventing unauthorized access, use, disclosure, interruption, modification or destruction of information in order to preserve its confidentiality, integrity/authenticity and availability.

In fact, in the field of research there are a reasonable number of studies on Information Systems Security and on the application of ISO/IEC 27002:2013, however, the number of studies applied to Local Governments in Portugal is practically non-existent, with this work aims to contribute to fill this gap.

This case study aimed to assess, through the application of a questionnaire survey based on ISO/IEC 27002:2013 associated with a maturity model, the maturity level of security controls of the Information System in the Municipality of Torres Novas.

The application of these two tools together allowed measuring the maturity level of security controls of the municipality's Information System and identifying quantitatively which areas are the most critical.

Keywords: Local Governments, ISO/IEC 27002:2013, maturity model, information security

Índice

Índice de Figuras

Índice de Tabelas

Índice de Gráficos

Lista de Abreviaturas e Siglas

CIA	Confidentiality, Integrity and Availability
CID	Confidencialidade, Integridade e Disponibilidade
COBIT	Control Objectives for Information and Related Technologies
COVID 19	Coronavirus disease 2019
CPU	Central Processing Unit
DGEEC	Direção-Geral de Estatísticas da Educação e da Ciência
DSECTSI	Direção de Serviços de Estatísticas da Ciência e Tecnologia e da Sociedade de Informação
DTICMA	Divisão de Tecnologias de Informação, Comunicação e Modernização Administrativa
ERP	Enterprise Resource Planning
GB	Gigabytes
I&D	Investigação e Desenvolvimento
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
IUTICCM	Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Câmaras Municipais
MTN	Município de Torres Novas
RGPD	Regulamento Geral sobre a Proteção de Dados
SGBD	Sistema de Gestão de Banco de Dados
SI	Sistemas de Informação
TIC	Tecnologias da Informação e da Comunicação

1 Introdução

1.1 Contextualização do Estudo

Numa Era em que todas as organizações lidam no seu dia a dia com informação dos seus colaboradores, fornecedores, parceiros, utilizadores, etc., esta tornou-se um ativo essencial, que precisa de ser adequadamente protegido.

> A informação é, hoje em dia, um dos motores da atividade humana. De facto, independentemente do tamanho, natureza ou mesmo atividade de uma organização, a verdade é que esta precisa de informação para poder executar e prosseguir a sua missão e cumprir os objetivos a que se propõe (Gouveia & Ranito, 2004, p. 5).

Para as Autarquias Locais, onde se verificam constantes mudanças nos processos organizacionais com o objetivo de uma melhor utilização económica, eficiente e equitativa dos recursos públicos, os Sistemas de Informação são um fator-chave. Ao lidarem diariamente com informação confidencial estão sujeitas a obrigações de conformidade ética e legal, que geram grandes responsabilidades na gestão da informação que tratam e produzem.

> Mesmo para organizações privadas a questão da segurança é um tópico bem atual. No caso das autarquias, a pressão é ainda maior, uma vez que tratam com dados muito sensíveis, oficiais e estão num processo de abrir comunicações eletrónicas com o cidadão/munícipe, criando portas de entrada potencialmente perigosas, se não forem devidamente acauteladas (Gouveia & Ranito, 2004, p. 91).

A par da evolução das tecnologias da informação e comunicação e da dependência crescente entre o bom funcionamento das organizações e o normal funcionamento dos Sistemas de Informação está o aumento da criminalidade informática, que se manifesta através de técnicas de intrusão e aproveitamento de vulnerabilidades, o que impõe melhorias aos paradigmas da segurança.

Beal (2005) refere que as organizações precisam adotar controlos de segurança (medidas de proteção que abranjam uma grande diversidade de iniciativas) que sejam capazes de proteger adequadamente dados, informações e conhecimentos.

A Segurança da Informação é conseguida através da implementação de um conjunto de controlos adequados (políticas, procedimentos, processos, estruturas organizacionais) que têm de ser estabelecidos, implementados, monitorizados, revistos e melhorados continuamente de forma a proteger o Sistema de Informação impedindo o acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados da informação, preservando a confidencialidade, integridade/autenticidade e disponibilidade da informação.

> Numa Sociedade que cada vez mais privilegia a informação como uma das suas preocupações mais dominantes, a necessidade de existir numa organização a infraestrutura adequada para a sua recolha, armazenamento, processamento, representação e distribuição faz com que uma parcela apreciável do esforço da organização seja tomada por estas preocupações (Gouveia & Ranito, 2004, p. 5).

Nos últimos anos tem-se verificado um desenvolvimento de normas e *frameworks*, reconhecidas internacionalmente, que definem princípios, conceitos, controlos e componentes de gestão de segurança de informação, que visam apoiar as organizações na implementação de um Sistema de Gestão de Segurança da Informação.

> As normas técnicas de boas práticas ou *standards* relacionados com as Tecnologias de Informação e Comunicação evoluíram para acompanhar a nova realidade dos Sistemas de Informação e estão a ser adotadas por muitas organizações. Estes novos *standards* técnicos ilustram procedimentos aceites generalizadamente que podem ser usados em auditoria como referenciais para avaliação comparativa de conformidade e controlo dos Sistemas de Informação e procedimentos instituídos (Pedro, 2010, p. 157).

Estas normas e *frameworks* são aplicáveis às Autarquias Locais, representam baixos custos e são uma ótima opção, pois podem ser aplicadas pelos recursos internos, não sendo necessário recorrer à contratação de serviços externos.

O Município de Torres Novas aplica um conjunto de controlos para garantir a Segurança da Informação, no entanto nunca aplicou um método para avaliar se os controlos de segurança do Sistema de Informação utilizados são os mais adequados, o que pode originar fraquezas e uma maior exposição ao risco.

Analisadas algumas das principais metodologias utilizadas na área de gestão de Segurança da Informação (ISO/IEC 27002:2013, COBIT e ITIL) concluiu-se que aquela que mais se adequava à realização deste trabalho é a ISO/IEC 27002:2013.

A ISO/IEC 27002:2013 é um código de boas práticas para a gestão da segurança dos Sistemas de Informação. Esta norma estabelece diretrizes e procedimentos para iniciar, implementar, manter e melhorar a gestão de segurança de uma organização e, em conjunto com um modelo de maturidade de segurança, permite medir a performance da Segurança da Informação nas organizações.

1.2 Objetivos do Estudo

1.2.1 Objetivo Geral

Com este estudo de caso pretende-se avaliar o grau de maturidade dos controlos de segurança do Sistema de Informação no Município de Torres Novas, permitindo identificar as melhorias necessárias, e incutir uma atitude de melhoria continua través da monitorização e verificação dos Sistemas de Informação.

1.2.2 Objetivos Específicos

Os objetivos específicos deste estudo de caso são:

- Efetuar uma análise de segurança aos controlos de segurança do Sistema de Informação do Município de Torres Novas baseada nos controlos previstos na norma ISO/IEC 27002:2013;
- Classificar o nível de maturidade dos controlos utilizando um modelo de maturidade de segurança;
- Apresentar resultados sob a forma quantitativa permitindo de forma simples identificar as áreas mais críticas.

1.3 Relevância do Estudo

No domínio da investigação observa-se a existência de um número razoável de estudos sobre Segurança de Sistemas de Informação e sobre a aplicação da ISO/IEC 27002:2013, contudo, o número de estudos aplicados a Autarquias Locais em Portugal é praticamente inexistente, com este trabalho visa contribuir-se para colmatar esta lacuna.

O Município de Torres Novas não possui um método de avaliação da adequação dos controlos de segurança do Sistema de Informação implementados, este facto pode levar a que os controlos adotados não sejam os ideais, originando uma maior exposição ao risco.

Este estudo irá contribuir para uma melhoria dos procedimentos atuais de proteção da informação no Município de Torres Novas, pois uma avaliação baseada na ISO/IEC 27002:2013 permite uma visão abrangente de todo o Sistema de Informação, possibilitando uma melhor perceção da adequação dos controlos utilizados e se necessário melhorá-los de forma a obter um Sistema de Informação mais robusto.

Esta avaliação pode também ser utilizada como suporte para a tomada de decisões relacionadas com melhorias e investimento necessários para assegurar a Segurança da Informação, bem essencial da organização.

1.4 Estrutura do Trabalho

O presente trabalho de investigação encontra-se organizado em seis capítulos.

No primeiro capítulo é efetuada uma breve introdução, onde se estabelece a contextualização, a problemática, o objetivo e a relevância do estudo.

No segundo capítulo é explanada a fundamentação do estudo, através da revisão da literatura, onde é abordado o estado de conhecimento sobre Sistemas de Informação, em particular na Administração Pública Local, a sua influência na auditoria, as principais Normas e Frameworks de Segurança de Informação e Modelo de Maturidade.

Por sua vez no terceiro capítulo é apresentada a organização em estudo, caracterizando-se a área de Tecnologias de Informação e Comunicação do Município de Torres Novas.

No quarto capítulo é exposta a metodologia adotada no projeto, são apresentados os instrumentos e técnicas de recolha de dados, bem como o procedimento de análise e tratamento dos dados.

No quinto capítulo são apresentados os resultados obtidos com a aplicação da ISO/IEC 27002:2013 associada ao Modelo de Maturidade e a respetiva interpretação.

Por fim, no sexto e último capítulo, são efetuadas as considerações finais, onde se apresenta a conclusão e as oportunidades para investigação futura

2 Sistemas de Informação na Administração Pública

2.1 Informação

Longe vai o tempo em que a grande preocupação das organizações eram apenas os seus ativos tangíveis (físicos e financeiros). O final do século XX, que ficou marcado por ser a Era da Informação (Vieira, 2019), trouxe importantes alterações a este nível, passando-se a valorizar a informação e a tecnologia.

A informação (todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa) passou a ser considerada uma fonte de poder, um ativo de elevado valor que deve ser adequadamente mantido e protegido.

Uma má utilização da informação ou a sua divulgação indevida "pode gerar danos e envolver ilícitos que vão desde a quebra de sigilo profissional a vazamento de informação confidencial de uma instituição, ou exposição de uma vida íntima ou privacidade de uma pessoa" (Pinheiro & Sleiman, 2009, p. 27).

Atualmente, com a quantidade de informação existente nas organizações, a sua produção e armazenamento só se torna economicamente viável através da utilização de sistemas informatizados, tornando-as assim, cada vez mais, dependente das Tecnologias de Informação e Comunicação.

Viver na Era da Informação significa estar mais acessível e, consequentemente, mais exposto. As comunicações são mais rápidas e dinâmicas, passando do âmbito local para o alcance global. O relacionamento entre pessoas passou a fazer-se *online*, gerando mudanças de hábitos e promovendo a comunicação através de troca de mensagens eletrónicas (Pinheiro & Sleiman, 2009).

A troca de informações entre as organizações, de qualquer tipo ou finalidade, intensificou-se através do meio eletrónico, principalmente com a chegada do comércio eletrónico e da disponibilização de serviços bancários online. A Internet passou a ser mais transacional e, cada vez mais, os bens das organizações passaram a ser representados de maneira intangível, ou seja, informações armazenadas em meios eletrónicos. O modelo de riqueza deixou de ser o de bens de produção e passou a ser o do conhecimento, de acordo com Pinheiro e Sleiman (2009).

A crescente necessidade de utilização massiva da Internet e dos serviços que lhe estão associados, das tecnologias de informação e comunicação, expõem as organizações a novas vulnerabilidades e ameaças, colocando-as diariamente perante novos riscos com elevado grau de sofisticação.

O número de ameaças que a informação está sujeita é cada vez mais elevado e consequentemente a necessidade de proteger os Sistemas de Informação tornou-se uma constante.

2.1.1 Classificação da Informação

Nem toda a informação é vital ou essencial para merecer cuidados especiais, é importante classificá-la, definir o seu nível de confidencialidade, integridade e criticidade de acesso (disponibilidade) de forma a que mantenha os seus requisitos fundamentais durante todo o seu ciclo de vida e se evite o desperdício de recursos numa informação que não necessite de tanta segurança.

A norma ISO/IEC 27002:2013[1] no seu ponto 8.2.1 refere que a classificação da informação tem como objetivo assegurar que a informação recebe um nível adequado de proteção, de acordo com a sua importância para a organização, devendo ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

A mesma norma recomenda que a classificação deve ser consistente em toda a organização de forma que cada pessoa possa classificar a informação e os ativos relacionados da mesma forma, e tenham um entendimento comum dos requisitos de proteção e apliquem a proteção apropriada, e que convém que os resultados da classificação sejam atualizados de acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida.

De acordo com a ISO/IEC 27002:2013 convém que os proprietários de ativos de informação sejam responsáveis pela sua classificação, e que os resultados da classificação

[1] ISO/IEC 27002:2013 – Information Technology – Security Techniques – Code of Practice for Information Security – Controls.

indiquem o valor dos ativos em função da sua sensibilidade e criticidade para a organização, em termos da confidencialidade, integridade e disponibilidade.

De facto, quem cria e manipula a informação é a pessoa mais habilitada para a classificar, por exemplo, um *chef* de cozinha que desenvolve uma nova receita. Para outra pessoa que veja a receita é apenas mais uma receita, mas para o *chef* é uma oportunidade de ser reconhecido e de poder ganhar muito dinheiro. Ou seja, o *chef* de cozinha classificará a informação ao nível mais alto de confidencialidade, mas provavelmente outra pessoa iria classificá-la como pública.

A ISO/IEC 27002:2013 não determina os níveis de classificação, cada organização deverá estabelecer os seus, de acordo com a sua realidade, quanto mais complexa a organização mais níveis de confidencialidade poderão existir, no entanto estabelece quatro níveis de classificação:

- **Nível 1 -** quando sua divulgação não causa nenhum dano;
- **Nível 2 -** quando a divulgação causa constrangimento menor ou inconveniência operacional menor;
- **Nível 3 -** quando a divulgação tem um pequeno impacto significativo nas operações ou objetivos táticos;
- **Nível 4 -** quando a divulgação tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

Os níveis apresentados na ISO/IEC 27002:2013 vão ao encontro dos níveis de classificação da informação mais comuns:

- **Informação Pública** - Pode ser disponibilizada, está acessível a qualquer pessoa sem causar danos, prejudicar a imagem ou integridade da organização.
- **Informação Interna** – Pode ser acedida apenas por colaboradores da empresa, embora as consequências do uso não autorizado não sejam um problema sério. Mesmo não sendo informações vitais o aspeto da integridade é importante (é o mais baixo nível de confidencialidade).

- **Informação Confidencial** - Acessível para um grupo de pessoas, a sua divulgação ou perda pode causar prejuízos (nível médio de confidencialidade).

- **Informação Restrita ou Secreta** - Acessível apenas para pessoas selecionadas, o acesso não autorizado a estas informações é extremamente crítico para a organização. A integridade dos dados é vital (o mais alto nível de confidencialidade).

Relativamente à classificação da informação a ISO/IEC 27002:2013 refere ainda que convém que os resultados da classificação sejam atualizados de acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida, isto porque a informação pode deixar de ser sensível ou crítica após certo período de tempo, por exemplo, quando a informação se torna pública. Convém que estes aspetos sejam levados em consideração, pois uma classificação superestimada pode levar à implementação de controlos desnecessários, resultando em despesas adicionais ou, pelo contrário, classificações subestimadas podem pôr em perigo o alcance dos objetivos de negócio.

Beal (2005) classifica ainda a informação quanto à disponibilidade e à integridade.

Relativamente à disponibilidade Beal (2005) refere que deve ser analisado o custo de produção, o custo de recuperação da informação e o impacto caso a informação seja completamente perdida.

A partir desta análise Beal (2005) classifica a informação definindo a exigência de disponibilidade e uma ordem de prioridade para a recuperação em caso de indisponibilidade:

- **Informação Vital:** é essencial para a sobrevivência da organização, cuja perda ou indisponibilidade por determinado período provoca prejuízos irreparáveis para os negócios;
- **Informação Crítica:** é aquela cuja perda ou indisponibilidade por tempo acima do determinado implica em sérios prejuízos para a organização;
- **Informação Comum:** é aquela cuja perda ou indisponibilidade por tempo acima do determinado não implica sérios prejuízos para a organização, dessa forma, não exige controlos rigorosos de contingência e recuperação como os aplicáveis às vitais e críticas.

Relativamente à integridade Beal (2005) refere que a falta de integridade da informação pode causas sérios danos para a organização e faz a seguinte classificação:

- **Informação com Alta Exigência de Integridade:** este tipo de informação se não estiver íntegra pode comprometer objetivos e trazer grandes prejuízos à organização, bem como descumprimento de leis;
- **Informação com Média Exigência de Integridade:** a falta de integridade neste tipo de informação não compromete nem gera grandes impactos à organização, mas pode causar prejuízos;
- **Informação com Baixa Exigência de Integridade:** este tipo de informação se não estiver íntegra pode facilmente ser detetada e não oferece risco considerável à organização.

2.1.2 Ciclo de Vida da Informação

A informação tem um ciclo de vida natural, desde a sua criação e origem, armazenamento, processamento, uso e transmissão, até a sua eventual destruição ou obsolescência. O valor e os riscos aos ativos podem variar durante o tempo de vida da informação (por exemplo, revelação não autorizada ou roubo de balanços financeiros de uma organização, é muito menos importante depois que elas são formalmente publicadas), porém a Segurança da Informação permanece importante em algumas etapas de todos os estágios (ISO/IEC 27002:2013).

Segundo a norma ISO/IEC 27002:2013 a organização deve identificar os ativos relevantes no ciclo de vida da informação e documentar a sua importância. Convém que o ciclo de vida da informação inclua a criação, o processamento, o armazenamento, a transmissão, a exclusão e a sua destruição.

Sêmola (2014) considera que o ciclo de vida da informação é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Destaca ainda que estes momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da empresa.

Para Sêmola (2014) o ciclo de vida da informação pode ser dividido em quatro etapas:

- **Manuseio** - Momento em que a informação é criada e manipulada, ao folhear um maço de papéis, ao digitar informações recém-geradas numa aplicação *Web* ou, ainda, ao utilizar a senha de acesso para autenticação, por exemplo.
- **Armazenamento** - Momento em que a informação é armazenada, seja numa base de dados partilhada, seja numa anotação de papel posteriormente arquivada, num CD-ROM, DVD-ROM ou *pen-drive* guardada na gaveta da secretária, por exemplo.
- **Transporte** - Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrónico, seja ao publicar num sistema *Web* ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo.
- **Descarte** - Momento em que a informação é descartada, seja ao depositar no caixote do lixo um material impresso, seja ao eliminar um ficheiro do seu computador ou, ainda, ao descartar um CD-ROM usado que apresentou falha na leitura.

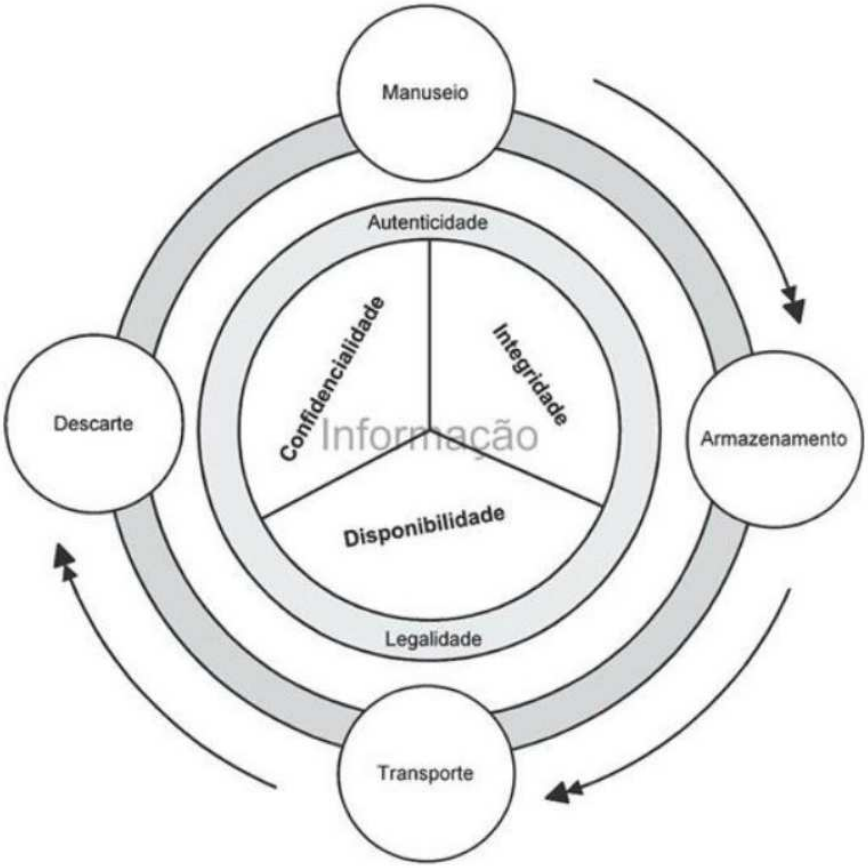

Figura 1: Ciclo de vida da informação considerando os conceitos básicos da informação e os aspetos complementares (Sêmola, 2014, p. 11)

As propriedades principais da informação (confidencialidade, integridade e disponibilidade) devem ser preservadas e garantidas durante todos os momentos do seu ciclo de vida.

Deve ser dado ao momento do descarte a mesma atenção que ao resto do ciclo, um descarte incorreto pode colocar toda a segurança em risco. Vejamos este exemplo dado por Sêmola (2014)**:**

> "Imagine...Você gera, em reunião, uma nova definição: informação estratégica confidencial. A mesma é anotada em papel e armazenada posteriormente em um cofre adequado. No momento imediatamente posterior, você incumbe a secretária de digitar tal informação e enviá-la por correio eletrônico aos envolvidos. Pense agora que, depois de completada a tarefa, a secretária não tenha adotado os procedimentos adequados de descarte e, consequentemente, tenha jogado, sem qualquer critério e tratamento, o material original em papel na lixeira mais próxima. Nesse exato momento, instaurou-se uma vulnerabilidade ou um furo de segurança! Agora imagine que haja efetivamente uma ameaça potencial pronta para explorar essa vulnerabilidade. Por exemplo: outro funcionário no perímetro físico da secretária, interessado, mas que não participara da reunião e tenha objetivos obscuros. Pronto! Por mais que tenha sido adotado um comportamento controlado e alinhado à política de segurança nos momentos de manuseio, armazenamento e transporte, a informação, alvo e motivo de todo o trabalho, esteve exposta no momento do descarte, comprometendo todos os demais e ainda pondo toda a segurança do negócio a perder." (Sêmola, 2014, p. 11).

Beal (2008), apresenta um ciclo de vida da informação mais desenvolvido, composto por sete etapas, representadas na figura 2: identificação das necessidades e dos requisitos, obtenção, tratamento, distribuição, uso, armazenamento e descarte.

- **Identificação das necessidades e dos requisitos,** é o ponto de partida do ciclo de vida da informação, funciona como o elemento acionador de todo o processo, podendo vir a estabelecer um ciclo contínuo de recolha de informação.
  "identificar as necessidades de informação dos grupos e indivíduos que integram a organização e dos seus públicos externos é um passo fundamental para que possam ser desenvolvidos serviços e produtos informacionais orientados

especificamente para cada grupo e necessidade interna e externa" (Beal, 2008, p. 5);

- **Obtenção**, o objetivo desta etapa é colmatar as necessidades de informação identificadas na etapa anterior, para isso "são desenvolvidas as atividades de criação, recepção ou captura de informação, proveniente de fonte externa ou interna, em qualquer mídia ou formato" (Beal, 2008, p. 5).

  Nesta etapa verifica-se uma preocupação acrescida com a integridade da informação, "é preciso garantir que a informação é genuína, criada por alguém autorizado a produzi-la (ou proveniente de uma fonte confiável), livre de adulteração, completa e apresentada dentro de um nível de precisão compatível com os requisitos levantados na etapa de identificação das necessidades" (Beal, 2008, p. 5).
- **Tratamento**, "é comum que a informação precise passar por processos de organização, formatação, estruturação, classificação, análise, síntese, apresentação e reprodução, para torná-la mais acessível, organizada e fácil de localizar pelos usuários" (Beal, 2008, p. 5).

  Nesta etapa a integridade da informação continua a ser uma preocupação, tem de ser mantida depois da informação ser tratada, a questão da confidencialidade começa também a ser relevante, é necessário garanti-la, sendo necessário ter em conta que podem existir cópias da informação aumentando assim o problema relacionado com as restrições de acesso.
- **Armazenamento**, assegura a preservação da informação, para que possa ser utilizada futuramente na organização. A preocupação com a integridade, disponibilidade e confidencialidade é uma constante nesta etapa, Beal (2008, p. 6) refere que "os objetivos de integridade e disponibilidade dos dados e informações armazenados podem adquirir maior destaque. A complexidade da conservação dos dados obviamente aumenta à medida que cresce a variedade de mídias usadas para armazená-los: bases de dados informatizadas, arquivos magnéticos ou ópticos, documentos em papel etc.".
- **Distribuição**, consiste em fazer chegar a informação a quem necessita dela, os utilizadores da informação podem ser internos ou externos, a eficiência desta etapa depende da qualidade da rede de distribuição.

Beal (2008, p. 6) refere que, nesta etapa, é necessário considerar "os diversos objetivos de segurança da comunicação, devendo ser analisados separadamente os requisitos de segurança relacionados aos processos de distribuição interna de informação daqueles voltados para a disseminação para públicos externos (parceiros, fornecedores, clientes, acionistas, grupos de pressão, governo etc.)".

- **Uso**, Beal (2008) considera esta etapa a mais importante de todo o ciclo de vida da informação pois, não é a existência da informação que garante bons resultados para uma organização, mas sim a sua boa utilização.

  Tal como na etapa de armazenamento a preocupação com a integridade, disponibilidade e confidencialidade é uma constante, devendo estes conceitos ser aplicados na sua plenitude.

  A necessidade futura de recuperação de dados é também uma preocupação a ter em conta nesta etapa.

- **Descarte**, Beal (2008) refere que quando uma informação se torna obsoleta ou perde a utilidade para a organização deve ser descartada, no entanto este descarte deve de ser realizado obedecendo a normas legais, políticas operacionais e exigências internas.

  A mesma autora considera também que, excluir dados e informações inúteis melhora o processo de gestão da informação a vários níveis (economiza recursos de armazenamento, aumenta a rapidez e eficiência na localização da informação necessária, melhora a visibilidade dos recursos informacionais importantes etc.).

  No entanto, salienta que, ao realizar o descarte é necessário ter em conta a confidencialidade e a disponibilidade da informação, relativamente à confidencialidade o descarte de dados e informações de caráter sigiloso tem que ser efetuado cumprindo critérios rígidos de destruição segura, garantindo que não podem ser recuperados, no que se refere à disponibilidade é necessário assegurar que as informações não vão ser exigidas no futuro e que os dados históricos valiosos para o negócio são preservados.

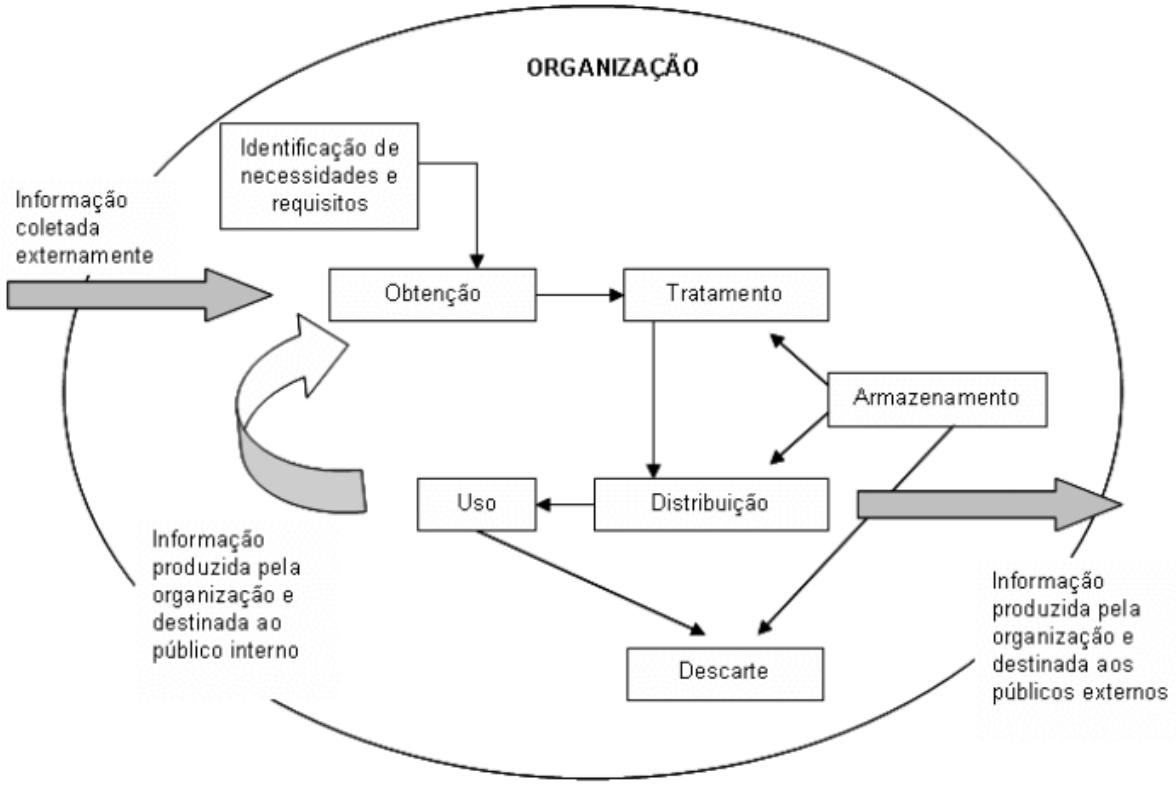

Figura 2: Representação do fluxo da informação nas organizações (Beal, 2008, p. 9)

2.2 Sistemas de Informação

Tendo todas as organizações uma necessidade constante de obter e produzir informação fiável que lhes permita gerir a sua atividade e alcançar os objetivos definidos. Sendo a informação um ativo de tão elevada importância para as organizações tem-se verificado o desenvolvimento de mecanismos para a sua gestão, através dos denominados Sistemas de Informação.

O'Brien e Marakas (2007, p. 4) consideram que "Sistema de Informação pode ser qualquer combinação organizada de pessoas, hardware, software, redes de comunicações, recursos de dados e políticas e procedimentos que armazenam, restauram, transformam e disseminam informações em uma organização."

Os Sistemas de Informação têm como elemento fundamental a informação, o seu objetivo é armazenar, tratar e disponibilizar informação que permite apoiar ou mesmo executar funções ou processos numa organização, ajuda ainda o administrador a tomar decisões baseadas em informações mais consistentes e precisas, além de facilitar o planeamento e controlo das tarefas.

As Tecnologias de Informação e Comunicação, das quais os Sistemas de Informação fazem parte, têm evoluído e são cada vez mais complexos. As tecnologias de informação e comunicação vieram proporcionar um aumento da eficiência nas organizações, nomeadamente ao nível do armazenamento e processamento da informação e da comunicação a distância.

Nos dias de hoje, os Sistemas de Informação, são essenciais ao bom funcionamento das instituições havendo mesmo uma dependência entre a atividade das organizações e o normal funcionamento dos Sistemas de Informação.

Esta crescente dependência dos Sistemas de Informação e das indispensáveis redes informáticas conduziu a um aumento das ameaças à confidencialidade da informação.

A possibilidade de ameaças por acesso indevido, abuso ou fraude, não fica limitada a um único lugar, podendo ocorrer em qualquer um dos pontos de acesso à rede.

Independentemente do tipo, da natureza (pública ou privada) ou da dimensão da organização, atualmente, a troca de informação assenta numa rede global, a Internet, o que aumenta a exposição dos Sistemas de Informação a novas ameaças.

Com o constante surgir de novas áreas e oportunidades de invasão e manipulação, a tendência é que as ameaças à Segurança da Informação continuem a crescer, não apenas em número de ocorrências, mas também em velocidade, complexidade e alcance. A Segurança da Informação tornou-se o um desafio permanente.

O'Brien e Marakas (2007) referem ainda que:

> um Sistema de Informação (SI) depende de recursos de pessoas (utilizadores finais e especialistas de Sistemas de Informação), *hardware* (máquinas e meios de armazenamento de dados), *software* (programas e procedimentos), dados (bases de dados e conhecimento) e redes (meios de comunicação e suporte de rede) para realizar entrada, processamento, saída, armazenamento e controlar as atividades que convertem os recursos de dados em produtos de informação (O'Brien & Marakas, 2007, p. 29).

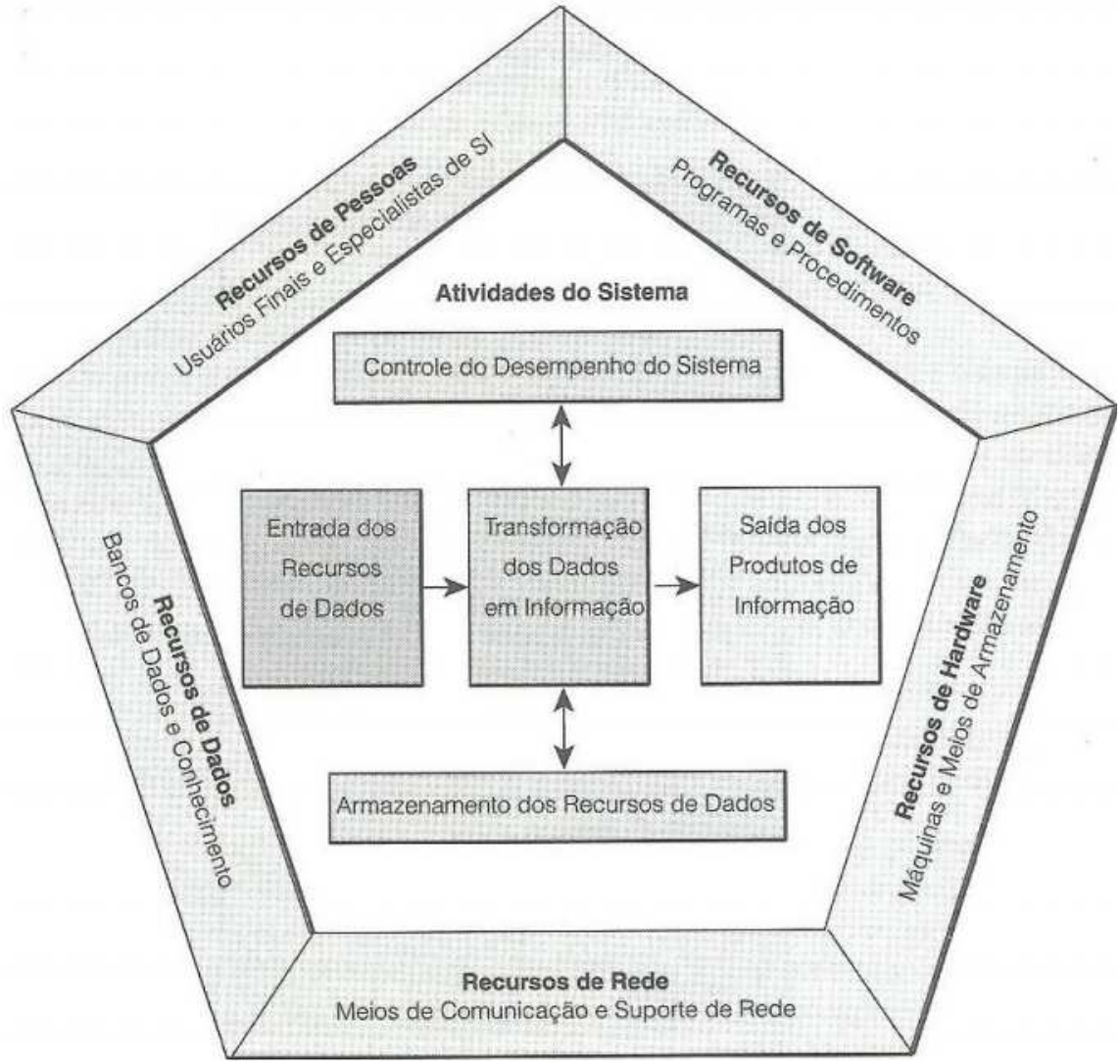

Figura 3: Componentes de um Sistema de Informação (O'Brien & Marakas 2007, p. 29)

Na figura 3 O'Brien e Marakas (2007) apresentam um modelo básico de Sistemas de Informação onde consta um conjunto de conceitos que consideram poderem ser aplicados a todos os sistemas:

1. Pessoas, *hardware*, *software*, dados e redes são os cinco recursos básicos dos Sistemas de Informação.

- Os **Recursos de Pessoas** incluem utilizadores finais e especialistas de Sistemas de Informação. Os utilizadores finais (também chamados utilizadores ou clientes) são as pessoas que usam um Sistema de Informação ou a informação que este produza. Os especialistas de Sistemas de Informação são as pessoas que desenvolvem e operam Sistemas de Informação.
- Os **Recursos de *Hardware*** consistem em máquinas e meios de armazenamento, incluindo todos os dispositivos físicos e materiais usados no processamento da informação, não apenas máquinas, mas também todo o meio de armazenamento de dados,

isto é, objetos tangíveis nos quais os dados são gravados, de folhas de papel a discos óticos ou magnéticos, impressoras, *scanners*, etc.

- Os **Recursos de *Software*** incluem todos os conjuntos de instruções e processamento de informação, não apenas os conjuntos de instruções operacionais chamados programas, que diretamente controlam o *hardware* do computador, mas também os conjuntos de instruções de processamento de informação chamados procedimentos de que as pessoas necessitam.
- Os **Recursos de Dados**, podem incluir bases de dados e bases de conhecimento, são a matéria-prima dos Sistemas de Informação, o sangue vital de organizações atuais, e a administração eficaz e eficiente dos dados. É considerado uma parte integrante da estratégia organizacional.
- Os **Recursos de Rede** incluem meios de comunicação e redes (são os meios de comunicação, processadores de comunicação, e programas de controlo e acesso à rede).

2. Em todos os Sistemas de Informação ocorrem as mesmas atividades básicas, a entrada, o processamento, a saída, o armazenamento de dados.

- **Entrada de Recursos de Dados**, os dados devem ser capturados e preparados para o processamento pela atividade de entrada. A entrada toma a forma de atividades de entrada de dados, como gravar e editar.
- **Processamento dos Dados em informação**, os dados são submetidos a atividades de processamento, como cálculo, comparação, ordenação, classificação e resumo. Essas atividades organizam, analisam e manipulam os dados e, assim, os convertem em informação para os utilizadores finais. A qualidade de quaisquer dados armazenados num Sistema de Informação deve ser também mantida por um processo continuo de atividades de correção e atualização.
- **Saída de Produtos de Informação**, a informação em diversas formas é transmitida aos utilizadores finais e disponibilizada na atividade de saída. O objetivo dos Sistemas de Informação é a obtenção de produtos de informação apropriados aos utilizadores finais.
- **Armazenamento dos Recursos Dados**, o armazenamento é um componente básico de um Sistema de Informação. O armazenamento é a atividade do Sistema de Informação na qual os dados são retidos de maneira organizada para uso posterior.
- **Controlo de Desempenho do Sistema**, uma atividade importante de um Sistema de Informação é o controlo do seu desempenho. Um Sistema de Informação deve fornecer *feedback* a respeito de suas atividades de entrada, processamento, saída e armazenamento. Esse *feedback* deve ser controlado e avaliado para determinar se o sistema está a atingir os padrões de desempenho estabelecidos.

Os Sistemas de Informação podem ser classificados de várias formas. O'Brien e Marakas (2007) classificam-nos de acordo com o papel que desempenham nas operações e na gestão de um negócio, dividindo-os em sistemas de apoio às operações, sistemas de suporte à gestão e outros sistemas.

Os **Sistemas de Apoio às Operações** processam dados gerados e utilizados nas operações de negócios, produzindo uma variedade de informação para uso interno e externo, o seu objetivo não é produzir informação específica para ser utilizada pela gestão na tomada de decisões, mas sim "processar eficientemente as transações de negócios, controlar os processos industriais, apoiar as comunicações e a colaboração, e atualizar bancos de dados corporativos" (O'Brien & Marakas, 2007, p. 14).

O'Brien e Marakas (2007) consideram, dentro dos sistemas de apoio às operações, três tipos de sistemas:

- Sistemas de Processamento de Transações – "registam e processam os dados resultantes das transações de negócios", por exemplo "sistemas de processamento de vendas e estoque e de contabilidade" (O'Brien & Marakas, 2007, p. 14).
- Sistemas de Controlo de Processos - monitorizam e controlam processos físicos industriais, por exemplo, uma refinaria de petróleo utiliza sensores eletrónicos ligados a computadores para monitorizar constantemente os processos químicos e fazer ajustes instantâneos (em tempo real) que controlam o processo da refinaria (O'Brien & Marakas, 2007, p. 14 e 15).
- Sistemas Colaborativos – apoiam a comunicação, a produtividade e a colaboração de equipa e de grupos de trabalho e "incluem aplicações que são às vezes chamadas sistemas de automatação de escritório." Por exemplo, "sistemas de e-mail, *chat* e videoconferência." (O'Brien & Marakas, 2007, p. 15).

Os **Sistemas de Suporte à Gestão** são "as aplicações do Sistema de Informação que se concentram em informar e dar suporte para a eficaz tomada de decisão por parte da gerência" (O'Brien & Marakas, 2007, p. 15).

O'Brien e Marakas (2007) apresentam três tipo de sistemas de suporte à gestão:

- Sistema de Informação de Gestão (MIS) - agrupam e sintetizam os dados das operações realizadas na organização para facilitar a tomada de decisão pelos

gestores “fornecem informações na forma de relatórios e telas a gerentes e muitos profissionais de negócios.” Por exemplo, “sistemas de relatórios de análise de vendas, desempenho da produção e tendência de custo” (O’Brien & Marakas, 2007, p. 15).

- Sistemas de Suporte à Decisão (DSS) – “dão suporte direto do computador aos gerentes durante o processo de tomada de decisão: um gerente de publicidade pode usar um DSS para executar uma análise de tipo “e se…” como parte de uma decisão para determinar onde investir o orçamento da publicidade. Um gerente de produção pode usar um DSS para decidir a quantidade de produtos a manufaturar baseado nas vendas esperadas associadas a uma futura promoção e na localização e disponibilidade das matérias-primas necessárias para manufaturar o produto” (O’Brien & Marakas, 2007, p. 15 e 16).

- Sistemas de Informação Executiva (EIS) – integram e sintetizam dados de fontes internas e externas à organização, utilizando para isso ferramentas de análise, simulação e comparação de forma a facilitar a tomada de decisão da gestão.

  “Fornece informação fundamental dos MIS, DSS e outras fontes adaptadas às necessidades de informação dos executivos. Exemplos: sistemas de fácil acesso a análises do desempenho dos negócios, ás ações dos concorrentes e aos desenvolvimentos econômicos para apoiar o planeamento estratégico” (O’Brien & Marakas, 2007, p. 15).

Existem ainda outras categorias de Sistemas de Informação que podem dar suporte às aplicações operacionais e gerenciais, O’Brien e Marakas (2007) referem os sistemas especialistas, os sistemas de gestão de conhecimento, os sistemas funcionais de negócio e os Sistemas de Informação estratégica.

> Os sistemas especialistas podem fornecer recomendação adequada a pequenas tarefas operacionais, como diagnóstico de equipamento, como a decisões administrativas, como gerenciamento de carteira de empréstimos. Os sistemas de gestão de conhecimento são Sistemas de Informação baseados no conhecimento que apoiam a criação, a organização e a disseminação do conhecimento de negócios a empregados e gerentes em toda a empresa. Os Sistemas de Informação que se concentram em aplicações operacionais e administrativas em apoio a funções básicas de negócio, como contabilidade ou marketing são conhecidos

como sistemas funcionais de negócio. Finalmente, os Sistemas de Informação estratégica aplicam a tecnologia da informação a produtos, serviços ou processos de negócios com uma firma para ajudá-la a obter vantagem estratégica sobre seus concorrentes (O'Brien & Marakas, 2007, p. 16).

Os mesmos autores salientam que "É também importante perceber que as aplicações de negócios dos Sistemas de Informação no mundo real são combinações em geral integradas dos vários tipos de Sistemas de Informação (…)", "Na prática são combinados em Sistemas de Informação integrados ou interfuncionais, que fornecem uma variedade de funções" (O'Brien & Marakas, 2007, p. 16).

Na figura 4 O'Brien e Marakas (2007) representam esquematicamente a classificação dos Sistemas de Informação.

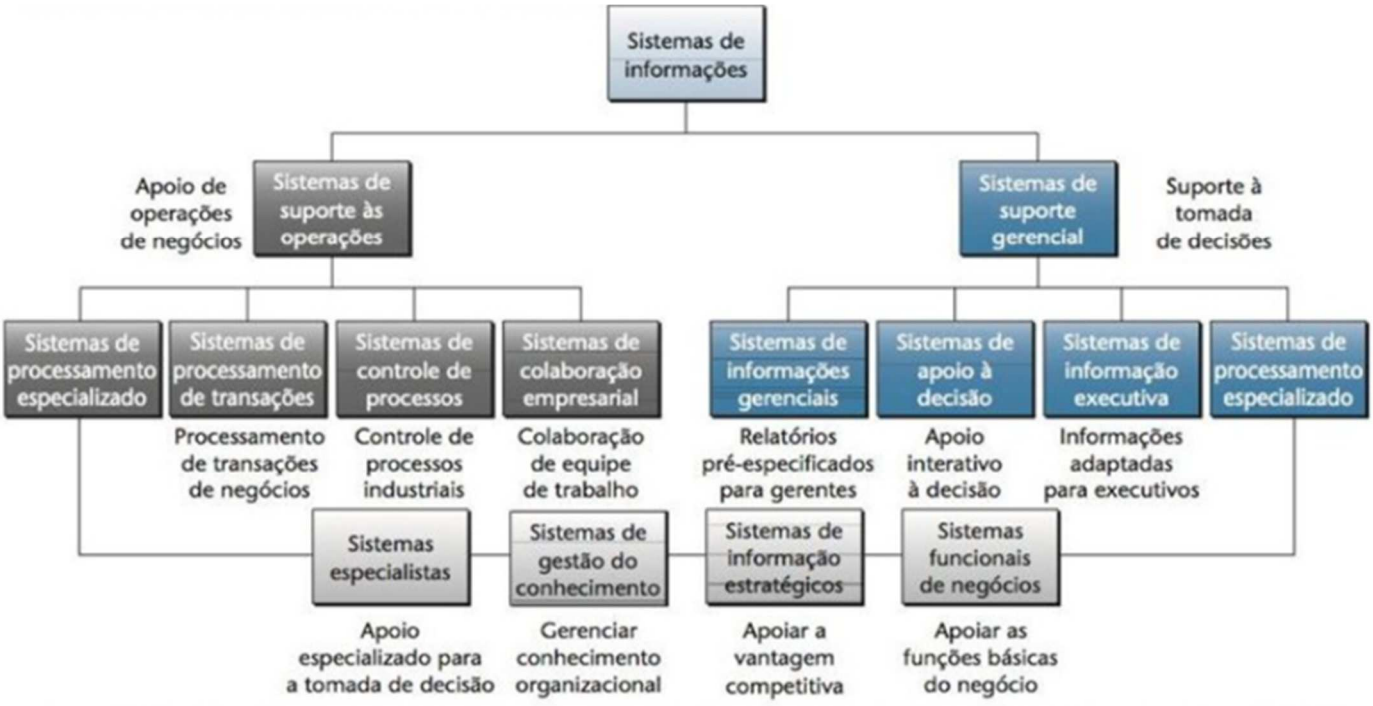

Figura 4: Classificação dos Sistemas de Informação (O'Brien & Marakas, 2007, p. 14).

2.2.1 Os Sistemas de Informação e a Auditoria

Como referido os Sistemas de Informação são, atualmente, imprescindíveis em praticamente todas as organizações. A rápida evolução das tecnologias de informação e comunicação levou à transição de registos manuais para processos informatizados, permitindo uma maior rapidez nas tarefas executadas diariamente e o tratamento e armazenamento de elevado volume de informação.

Para Borges, Rodrigues e Rodrigues (2010, p. 134)

> a comprovada necessidade de tratamento de grande volume de dados que visam proporcionar informação fiável, e em tempo útil, para a tomada de decisão a diversos níveis, conjugada com os avanços vertiginosos conseguidos no domínio da informática, revolucionaram os processos clássicos de escrituração, subalternizando os respetivos fundamentos teóricos.

Acerca da informatização dos processos Pedro (2010, p. 159) refere que

> Antes da automatização era suficiente analisar a documentação e perguntar aos empregados o que faziam para conhecer os circuitos da informação e os procedimentos instituídos numa organização. Por vezes, os impressos usados constituíam um bom ponto de partida para conhecer a ramificação dos circuitos através das cópias e as responsabilidades através das assinaturas.

Como consequência Pedro (2010, p. 159), refere ainda que

> Hoje é necessário avaliar os meios eletrónicos associados ao processamento de informação relativa aos procedimentos automáticos. Isto é, os circuitos de comunicações, os repositórios, o software e o hardware passaram a ter significado funcional em auditoria. Os circuitos, os procedimentos e as responsabilidades, não estão documentados. Estão embebidos em software que é impossível ler na grande maioria das vezes.

Esta evolução tecnológica teve um significativo impacto no processo de auditoria, atualmente o auditor necessita de expressar uma opinião baseada em grandes volumes de informação, que se encontra envolta numa complexa estrutura em constante mudança (Marques, 2016).

Num processo de auditoria tradicional a utilização de tecnologia ocorria em menor escala, a informação circulava e era armazenada em suporte papel, as provas de auditoria eram obtidas essencialmente em suporte físico (Marques, 2016). O auditor necessitava igualmente de conhecer pormenorizadamente os circuitos da informação, mas a sua identificação e visualização era mais fácil, através da observação e do diálogo com os intervenientes em cada fase dos processos.

Atualmente os circuitos de informação flexibilizaram-se, tornaram-se virtuais, estão submersos nas redes informáticas, em *hardware* e *software* sofisticado, sendo necessário conhecer convenientemente o seu funcionamento.

O auditor tem que se adaptar a um ambiente incerto, a utilização das tecnologias de informação e comunicação faz agora parte do seu dia a dia, tendo de enfrentar assim novos desafios relacionados com a fiabilidade nos dados recolhidos a partir dos Sistemas de Informação, sendo necessário adaptar o modelo da auditoria à Era digital e do eletrónico.

De acordo com Costa (1998, p. 131):

> Os procedimentos de auditoria ao redor do computador deram então origem aos procedimentos de auditoria através do computador o que obrigou alguns auditores a especializarem-se fortemente na área de conhecimentos designada por auditoria informática, a qual se dirige a dois aspetos distintos: o controlo interno e as rotinas de informação contabilística e de gestão a nível operacional.

Segundo Oliveira (2005), a obtenção de evidência eletrónica é tecnicamente mais complexa, os dados são mais suscetíveis de ser alterados (intencionalmente ou não), a informação é mais difícil de visualizar e de verificar a sua origem (...) requerendo novos géneros de controlos preventivos e de sistemas de segurança.

Segundo Pedro (2010, p. 172)

> Os processos e os dados a auditar estão agora no centro de um conjunto de círculos tecnológicos constituídos por hardware, software de sistema, software aplicacional, redes de comunicação de dados e finalmente os próprios utilizadores dos sistemas. Cada um destes círculos pode condicionar a eficácia do controlo interno das organizações e coloca uma grande variedade de obstáculos à ação do auditor.

O mesmo autor representa esquematicamente esta visão na figura 5:

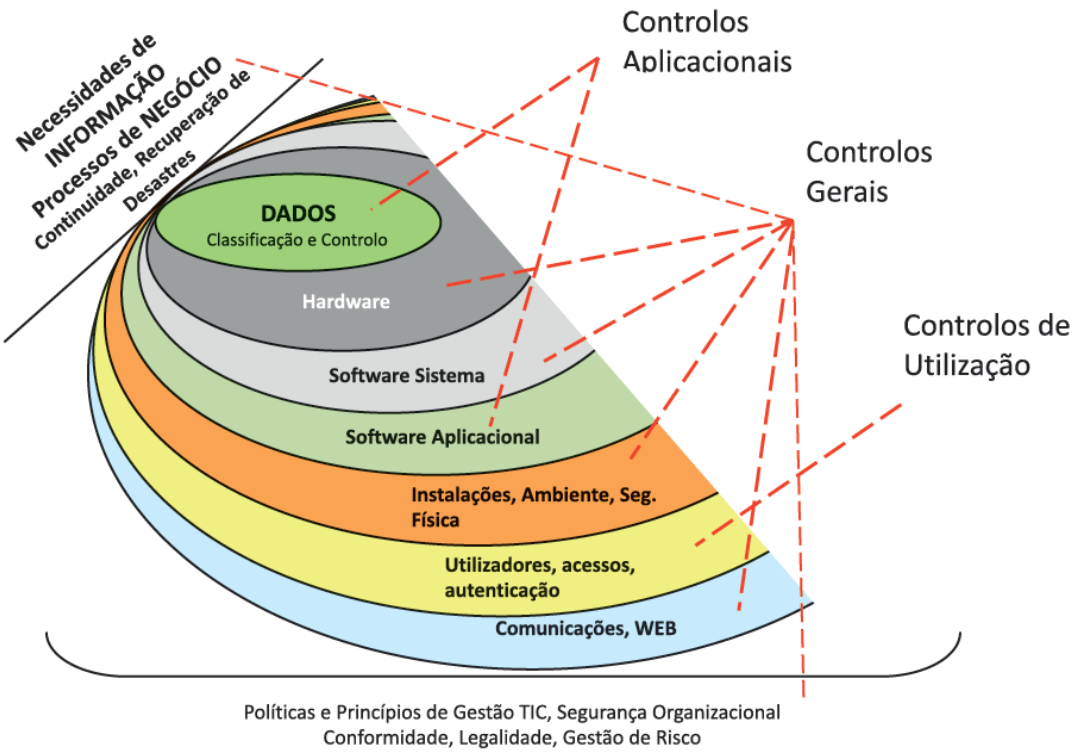

Figura 5 - Controlo Interno em Sistemas de Informação (Pedro, 2010, p. 173)

Marques (2013, p. 11) refere que:

> Os controlos aplicacionais têm como grande objetivo a proteção dos dados. São estes que averiguam se os dados preparados para inserir são completos, válidos e fiáveis; se os dados foram inseridos informaticamente de forma completa, precisa e atempadamente; se o seu processamento utilizou a aplicação correta, no devido tempo e segundo os requisitos estabelecidos; e se o output está protegido de modo a evitar alterações não autorizadas ou de dano e que se encontra distribuído conforme as políticas definidas.

Relativamente aos controlos gerais Marques (2013, p. 11) considera que estes se referem:

> essencialmente à estrutura organizativa e aos métodos e procedimentos determinados para regular a relação entre Sistemas de Informação informatizados com os demais elementos da empresa. A referir ainda que a eficácia dos controlos gerais está relacionada com a eficácia dos controlos aplicacionais. Ou seja, caso os controlos gerais sejam fracos, isso implicará uma diminuição considerável da fiabilidade dos controlos associados com as aplicações individuais, uma vez que significa que há o risco de facilmente poderem ser alvo de modificações ou que

são facilmente contornáveis. É por esta razão que, normalmente, os controlos gerais são avaliados antes e separadamente dos controlos de aplicação.

No que se refere aos controlos de utilização, tendo em conta a atual facilidade em aceder à informação, visam sobretudo avaliar a segurança na utilização da informação, a forma como são cedidos e segregados os acessos à mesma.

Pedro (2010, p. 168) considera que:

> Alguns autores arrumam os controlos apenas em duas categorias, controlos gerais e controlos aplicacionais não destacando os controlos de utilização. Optamos por destacar os controlos de utilização porque tratam do comportamento das pessoas que consideramos extremamente importante para o controlo. Se um controlo disparar um aviso e um utilizador dos sistemas não lhe ligar estamos perante um problema sério para todo o sistema de controlo.
>
> (…) os utilizadores dos sistemas são o último círculo envolvente da informação, aparentemente o menos tecnológico de todos, mas cada vez mais importante. Nenhum sistema é inteiramente automático, todos têm alguma intervenção humana. Se um funcionário decide escrever a sua password de acesso ao sistema na secretária ou num papel colado ao ecrã, podemos dizer que provavelmente será impossível garantir a autenticidade e a confidencialidade das transações contidas nesses sistemas.

O uso generalizado dos meios tecnológicos no processamento da informação veio colocar o auditor perante uma nova preocupação, a fiabilidade dos documentos.

Pedro (2010, p. 160) considera que antes de utilizar os dados em auditoria é necessário determinar a sua fiabilidade, sendo possível encontrar quatro situações:

- **Dados Fiáveis**: com base nos testes e análise efetuados concluímos que os dados são suficientemente credíveis para serem usados nos objetivos da missão de auditoria;
- **Dados Não Fiáveis, mas Utilizáveis**: os resultados dos testes efetuados aos circuitos mostraram uma taxa de erros que levanta dúvidas quanto à validade dos dados. Contudo, quando estes dados são vistos em contexto com outra evidência disponível, as opiniões, conclusões e recomendações extraídas através deles são válidas;

- **Dados Não Fiáveis nem Utilizáveis**: os resultados dos testes efetuados aos circuitos e aos dados mostraram uma taxa de erros que levanta dúvidas quanto à sua validade. Como os objetivos da missão requerem afirmações específicas baseadas nestes dados e não existe evidência adicional suficiente, somos incapazes de produzir projeções específicas, conclusões ou recomendações;
- **Fiabilidade Não Determinada**: Não estabelecemos a fiabilidade destes dados por isso, somos incapazes de produzir projeções específicas, conclusões ou recomendações baseadas nestes dados.

Pedro (2010, p. 159) refere ainda que

> Hoje, é tão fácil reproduzir documentos sobre papel a partir de dados armazenados em suporte eletrónico que não podemos aceitar como fiável um documento em papel sem analisar os circuitos dos dados que o produziram e o próprio papel. Antes da generalização dos suportes eletrónicos era mais difícil reproduzir documentos, as fotocopiadoras tinham limitações de cor e de composição, por isso era aceite a sua fiabilidade sem objeções

Consequência da utilização generalizada das tecnologias de informação e comunicação o auditor teve de adaptar e alterar os seus métodos de trabalho e metodologias à nova realidade. Pedro (2010, p. 163) apresenta uma síntese das alterações às metodologia, documentos e ambiente de trabalho do auditor:

Metodologias:

- Os princípios de controlo interno são válidos em todos os sistemas, quer sejam manuais, mecânicos ou eletrónicos, mas têm de ser avaliados com instrumentos diferentes em sistemas eletrónicos;
- Os procedimentos deixaram de ser manuais e passaram a ser executados por *software*. O auditor tem de observar a infraestrutura de comunicações, o *software* envolvido (Sistema operativo, SGBD, Programas, etc.), o *hardware* e as pessoas que intervêm na operação do sistema;
- Os circuitos de informação estão submersos em tecnologia e são desconhecidos das pessoas que intervêm nas transações;

- Há tecnologias adicionais que obrigam ao uso de conhecimentos, técnicas e procedimentos diferentes em qualquer das fases da auditoria, embora o modelo conceptual de abordagem se mantenha;

Documentos:

- O suporte eletrónico tende a evoluir para ser mais usado nos documentos;
- A autenticidade do documento depende da assinatura eletrónica;
- Os meios de escrita e leitura dos documentos são mais sofisticados, deixaram de ser apenas o lápis ou a caneta;
- O meio de circulação dos documentos já não é apenas o avião, o carro ou o carteiro, mas também o fio telefónico ou o espaço;
- A cópia dos documentos é milhares de vezes mais rápida e mais fácil do que em papel;
- O armazenamento dos documentos foi extraordinariamente facilitado;
- Os meios de pesquisa de conteúdos relevantes para a auditoria são rapidíssimos e eficientíssimos;
- Os documentos podem deixar vestígios e podem ser seguidos através da rede e dos servidores;
- Foi dificultada a possibilidade de seguir os registos de uma transação desde a sua ocorrência até ao montante refletido nas demonstrações financeiras ou em documento final idêntico;
- Os mecanismos de controlo do ciclo de processamento nos servidores e nas bases de dados nem sempre estão ativos de forma adequada e por isso não registam os acessos e outros acontecimentos em *log*.
- A documentação tende a ficar dispersa por vários locais de *input* devido às facilidades de transporte eletrónico dos dados;
- Ausência de documentos de *input* devido ao registo direto das transações no ecrã;
- Encontram-se por vezes totais de razão contabilístico acumulados sem valores parciais, por razões de economia de espaço, dificultando a identificação dos momentos subjacentes à transação.

Trabalho do Auditor:

- Ajuda a Auditoria – economia de tempo (ex.: auto de declarações pode ser feito, alterado e assinado logo no momento);
- Elaboração de relatório é mais rápida e este é mais fácil de alterar;
- Os testes substantivos podem ter mais volume de dados: possibilidade de abranger uma amostra estatística alagada. Pode reduzir a probabilidade de erro nos testes substantivos. Facilidade de análise;
- A seleção de amostras é mais fácil com base em valores ou outros atributos em cada rubrica;
- No controlo interno – se os perfis estiverem bem elaborados e se forem registados nos dados no momento de autorização os sistemas são mais fiáveis;
- Os papéis de trabalho e o arquivo são mais fácil de lidar;
- Melhora o planeamento de auditoria porque temos acesso a mais informação e podemos obter elementos à distância;
- Nos testes substantivos, as diferenças decorrem dos meios envolvidos no sistema auditado e nos instrumentos utilizados pelo auditor. O auditor pode copiar o *software* do sistema e os respetivos dados e reprocessar algumas ou todas as transações;
- A prática de amostragem é mais fácil, tal como a verificação de atributos nos documentos eletrónicos.

Por sua vez, também Sousa (2013) e Guedes (2010) referem riscos específicos que o uso das Tecnologias de Informação e Comunicação comportam, tais como:

- Confiança em sistemas ou programas que estão a processar dados incorretamente, ou a processar dados incorretos, ou ambos;
- Acesso não autorizado a dados que possa resultar na destruição dos dados ou alteração inapropriada dos mesmos, incluindo gravar transações não autorizadas, inexistentes ou incorretas;
- Alteração não autorizada aos dados dos ficheiros principais;
- Alteração não autorizada aos sistemas ou programas;
- Falhas na realização de alterações necessárias para a manutenção dos sistemas ou programas;
- Intervenção humana inapropriada;

- Possibilidade de perda de dados ou incapacidade de aceder aos dados como exigido.

Esta realidade implica a introdução de questões específicas, que podem conduzir a alterações na abordagem da auditoria.

Marques (1997) considera que as Tecnologias de Informação e Comunicação também trouxeram novas exigências, novos problemas, novos riscos e novas ameaças.

O objetivo e âmbito de uma auditoria não se alteram quando esta é efetuada em ambiente de tecnológico, o que muda são os procedimentos e os métodos utilizados pelos auditores, que têm que se adaptar a este novo contexto e adquirir competências técnicas a nível de Tecnologias de Informação e Comunicação.

> Quando um auditor entender que não possui os conhecimentos informáticos adequados à realização de determinados procedimentos que o auxiliem na efetivação do seu exame, não deve hesitar em se socorrer de um técnico de informática independente em relação à empresa objeto de auditoria, devendo, contudo, ter em atenção que nunca pode delegar as suas responsabilidades no que concerne à expressão do seu parecer (Costa, 1998, p. 132).

Também Pinto (2011) salienta que mesmo com a introdução dos computadores nas empresas, os objetivos da auditoria permanecem iguais, o que muda são os procedimentos e os métodos de que a auditoria se deve servir para se adaptar a este novo contexto, trata-se de adaptar o modelo da auditoria à nova realidade.

Podemos concluir que, com a utilização das Tecnologias de Informação e Comunicação surge a necessidade de confirmar que todos os dados informáticos sobre os quais o auditor está a incidir a sua análise se encontram corretos ou completos, sob o risco de todo o trabalho ser suportado em dados que não são os corretos e não servem de prova de auditoria, colocando em causa a opinião expressa.

2.2.2 Os Sistemas de Informação na Administração Pública Local

Nas últimas décadas do século XX assistiu-se ao despontar da preocupação com o cidadão enquanto "cliente" da Administração Pública. Esta preocupação surge associada à necessidade de modernizar e reformar a Administração Pública e ao movimento

denominado Nova Gestão Pública (*New Public Management*), cujas linhas estratégicas, resumidamente, são:

- Orientar a Administração Pública para as necessidades dos cidadãos;
- Abrir a Administração Pública à sociedade;
- Aumentar a sua eficiência;
- Evitar a corrupção;
- Torná-la mais transparente e idónea;
- Definir e identificar competências e responsabilidades;
- Evitar o desperdício.

A orientação para os clientes (internos e externos) tornou-se um ponto incontornável na modernização administrativa. Vidigal (1992) afirma que, de uma informática orientada exclusivamente para os processos internos de trabalho e centrada sobretudo em preocupações de natureza tecnológica, assistimos hoje ao despertar de novas tecnologias orientadas para os clientes.

As novas oportunidades criadas pela Sociedade da Informação vieram exigir da Administração Pública a adoção de novos paradigmas, novas estratégias e novas perspetivas quanto ao futuro.

São exigidos às organizações níveis de desempenho cada vez mais elevados, o mesmo acontece com a Administração Pública, prestadora de serviços por excelência e com um leque de clientes que será seguramente um dos mais numerosos.

A otimização dos serviços prestados torna-se uma necessidade pois o cidadão espera maior eficácia, flexibilidade, inovação, transparência, equidade, centralização e automatização dos serviços prestados.

"A tecnologia é cada vez mais um poderoso auxiliar para o processo decisório e um acelerador dos processos administrativos, aumentando o seu grau de certeza, transparência, imparcialidade e auditabilidade" (Vidigal, 2013, p. 470).

A Administração Pública no geral, e a Local em particular, tomam consciência das novas oportunidades criadas pelas Tecnologias de Informação e comunicação, sentindo a necessidade de diminuir, ou mesmo acabar, com os papeis, associados à burocracia. Neste sentido as Tecnologias de Informação e comunicação têm um papel estruturante e

facilitador, permitindo desencadear novos modelos de organização e novos processos de trabalho. Também o desenvolvimento das redes alargadas de informação (em particular da Internet) vieram criar oportunidades para fazer chegar ao cidadão toda a informação de que ele necessita no dia a dia.

No entanto, para conseguir aderir às novas Tecnologias de Informação e Comunicação a Administração Pública depara-se com uma grande dificuldade, a inexistência de arquiteturas de Sistemas de Informação, sendo requisito essencial conhecer detalhadamente os processos e a informação que circulam na organização, a estrutura interna e o circuito de decisão municipal.

Conforme Cardoso (2014, p. 25) refere é:

> a oportunidade que os Governos têm de impulsionar a reforma dos serviços em duas vertentes principais, provocando uma relação causa efeito: por um lado, a reorganização de todo o *back-office* que sustenta o conjunto de serviços, potenciando o surgimento de novos paradigmas de gestão da informação e, por outro, a definição de um novo *front-office* com a implementação de novos serviços e adaptação de antigos, disponibilizando aos cidadãos novos canais de comunicação com a Administração Pública.

É necessário rever a estrutura organizacional, adaptar os métodos de registo e comunicação, simplificar e racionalizar os procedimentos existentes, reajustar os fluxos de informação, uniformizar os modelos de documentos e transformá-los em formato eletrónico, sempre com o objetivo de tornar os serviços mais acessíveis e adaptados à comunidade local, melhorando a interação com os munícipes.

> (…) mais do que a tecnologia é a oportunidade de modernizar o *back-office*, em especial, da Administração Pública Local que está em jogo. Tal significa também a oportunidade para reinventar o próprio papel que esta detém face ao território que serve, nomeadamente (...) transformando serviços: tornando os serviços mais acessíveis, mais fáceis de usar e adaptados à comunidade local.
>
> Um dos seus objectivos gerais é melhorar a experiência de interacção com o indivíduo e assegurar a facilidade de partilha de informação com todos aqueles que o pretendam (munícipes e empresas locais, cidadãos, munícipes deslocados,

> turistas, instituições exteriores ao território, nomeadamente outros órgãos do poder local e central), (Gouveia, 2004, p. 27).

A modernização da Administração Pública, em particular da Local, veio implicar uma mudança da cultura organizacional, um desafio complexo, de grandes proporções, que envolve um elevado esforço de mudança e a aquisição de novas competências por parte dos funcionários, políticos e, até mesmo, dos munícipes.

> O sucesso da Administração Publica depende da sua capacidade para requalificar as suas antigas funções para os novos desafios da era digital, não se tratando apenas de mera mudança de tarefas de rotina para tarefas especializadas, mas, sobretudo, da criação de estruturas organizacionais e estilos de gestão favoráveis a esta transformação (Cardoso, 2014, p. 8).

Os Sistemas de Informação passam a assumir uma função de destaque, tornando-se a peça fundamental para a modernização administrativa da Administração Pública Local, contribuindo para a melhoria da qualidade e eficiência dos serviços prestados, aumentando substancialmente o potencial relacional como munícipe.

Consequentemente, os Sistemas de Informação passaram constituem a infraestrutura que suporta todo o fluxo de informação, internamente entre os funcionários com diferentes funções e responsabilidades e destes com o exterior.

À semelhança do que acontece no privado, com a progressiva desmaterialização dos processos e dos dados que os suportam, também a Administração Pública Local verifica uma dependência cada vez maior em relação às Tecnologias de Informação e Comunicação, sendo necessário reconhecer a importância e os riscos associados.

> Torna-se evidente a necessidade de salvaguardar as regras, os processos e os dados, que estão a ser cada vez mais desmaterializados e embebidos em tecnologias, constituindo eles próprios os verdadeiros ativos das organizações, (Vidigal, 2013, p. 475).

2.3 Segurança da Informação

Sendo a informação, no século XXI, um dos ativos mais precioso de uma organização, a sua segurança tornou-se uma prioridade que requer uma gestão adequada de forma a garantir que as suas propriedades fundamentais são mantidas permanentemente.

Para Sêmola (2014) Segurança da Informação é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade, Beal (2005) define a Segurança da Informação como o processo de proteger a informação das ameaças à sua integridade, disponibilidade e confidencialidade.

A ISO/IEC 27000:2018 refere que a Segurança da Informação garante a confidencialidade, disponibilidade e integridade da informação. A Segurança da Informação envolve a aplicação e a gestão dos controlos apropriados que envolvem a consideração de uma ampla variedade de ameaças, com o objetivo de assegurar o sucesso e a continuidade sustentáveis dos negócios e minimizar as consequências dos incidentes de Segurança da Informação.

Segundo ISO/IEC 27002:2013, a Segurança da Informação é alcançada pela implementação de um conjunto adequado de controlos, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de hardware e software.

Independentemente da definição atribuída, quando se fala em Segurança da Informação, é essencial referir a tríade CID ou, em inglês, CIA (*Confidentiality, Integrity and Availability*), também designada como a tríade da Segurança da Informação, composta pelas três propriedades fundamentais da informação: confidencialidade, integridade e disponibilidade que são a base de todo o conceito que garante a segurança de qualquer informação.

Figura 6: Tríade CID

É comum, a estas propriedades, encontrar associadas outras, tais como Autenticidade e Não Repúdio.

Na literatura especializada é possível encontrar diversas definições para as propriedades da informação, sendo, contudo, consensual que:

- **Confidencialidade:** é a garantia de que somente pessoas autorizadas terão acesso à informação, protegendo-a de acordo com o grau de sigilo do seu conteúdo. É a proteção dos Sistemas de Informação de forma a impedir que pessoas, ou equipamentos, não autorizadas tenham acesso ao mesmo.

  A ISO/IEC 27000:2018 refere que Confidencialidade é a propriedade em que as informações não são disponibilizadas ou divulgadas a pessoas, entidades ou processos não autorizados.
- **Integridade:** tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas não possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental. A informação não pode ser alterada, tem de se manter em tudo idêntica à sua forma original, durante todo o seu ciclo de vida.

  De acordo com a norma ISO/IEC 27000:2018, a Integridade deve ser entendida como propriedade de exatidão e completude.

  Existem definições que associam à Integridade as propriedades de Autenticidade Legalidade e Não-Repúdio, em que **Autenticidade** é a garantia de que a informação ou utilizador da mesma é autêntico, sendo possível atestar com

exatidão, a origem do dado ou informação, **Legalidade** é a garantia de que todas as informações estão de acordo as cláusulas contratuais acordadas ou a legislação nacional e internacional vigentes, por fim o **Não Repúdio** é a garantia de que o emissor de algum dado ou informação ou o autor de alguma ação sobre a informação não possa posteriormente negar que tenha enviado ou alterado algum dado/informação, é garantir que existem provas caso seja necessário provar "quem fez o quê".

- **Disponibilidade**, garante que a informação está a acessível e utilizável, em tempo útil, quando solicitada por pessoa, sistema, entidade ou órgão autorizado.
  A norma ISO/IEC 27000:2018 considera-a propriedade de ser acessível e utilizável quando solicitada por uma entidade autorizada.
  Possuir a informação necessária, mas não a ter disponível no momento adequado equivale a não possuir qualquer informação (Silva, Torres & Carvalho, 2003).

A tríade CIA deve ser complementada com uma outra tríade constituída por pessoas, processos e tecnologia (Pilares da Segurança da Informação).

Qualquer sistema de Segurança da Informação não envolve apenas tecnologia, por mais sofisticada que esta seja será apenas um elemento, sendo necessário envolver todos os componentes da organização, pessoas processos e tecnologia.

O segredo do sucesso de um sistema de Segurança da Informação está em conseguir equilibrar estes três elementos essenciais e intrinsecamente relacionados no contexto organizacional, em que as pessoas são o elemento formador da cultura organizacional e responsável por tornar o planeamento real, os processos são veículos informacionais que servem de guia às ações das pessoas e as tecnologias são as ferramentas que sustentam os processos.

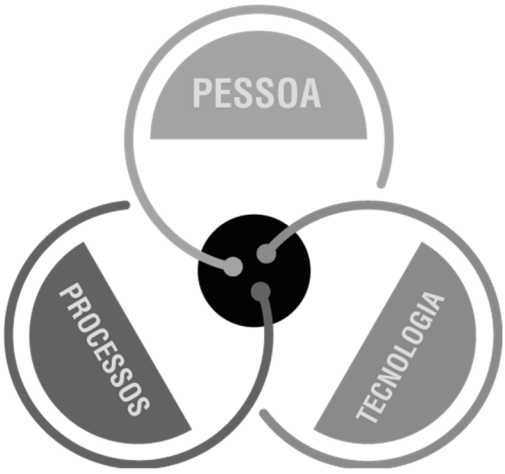

Figura 7: Pilares da Segurança da Informação (adaptada de: Life apps, 2020)

- **Pessoas:** As pessoas são o elemento central de um sistema de Segurança da Informação, são elas que executam e suportam todos os processos de uma organização, são o seu "elo mais fraco".

  Por muito bem projetado que seja o sistema de Segurança da Informação ele depende das pessoas para implementá-lo, ou seja, embora estas sejam o elo mais fraco e mais complexo da corrente tem de ser considerado para que a implementação tenha sucesso.

  Para Beal, (2008, p. 71) "qualquer esquema de segurança, por mais sofisticado que seja, pode ser derrubado pela atuação de uma única pessoa que decida abusar de seus privilégios de acesso e dados ou instalações de processamento da informação". Os incidentes de segurança envolvem sempre pessoas, quer do lado das vulnerabilidades exploradas, quer do lado das ameaças que exploram essas vulnerabilidades.

  Outro aspeto importante relacionado com o elemento pessoas é a engenharia social. A engenharia social é uma modalidade de ataque em que agentes mal-intencionados, valendo-se da ingenuidade, ignorância ou confiança dos utilizadores roubam informações de alto valor.

  Como refere Frisch (2002) a segurança tem início e termina com as pessoas.

- **Processos:** são um importante elemento para sustentar a Segurança da Informação, a vulnerabilidade deste pilar é responsável por gerar muitos dos incidentes de segurança, são o elemento integrador de todos os componentes da

organização (pessoas, papeis, responsabilidades, políticas, regras, estrutura organizacional e tecnologias de informação e comunicação).

Os processos são as atividades e ações organizadas de forma ordenada para que cada pessoa compreenda o que precisa de fazer, quando precisa de fazer e quais os resultados esperados, são como mapas que guiam as pessoas aos resultados desejados, são as diretrizes que organizam as ações das pessoas. Processos bem definidos são muito importantes, quando uma pessoa chave é substituída, reduzem a curva de tempo de aprendizagem e permitem que as atividades não fiquem comprometidas.

A correta gestão dos processos, numa organização, é essencial na proteção da informação. Processos bem definidos tornam a Segurança da Informação uma responsabilidade de todos e não só da equipa de segurança.

- **Tecnologia:** a maioria das organizações utiliza recursos tecnológicos para armazenar as suas informações e dados, a sua utilização já não é uma questão de opção, tornou-se indispensável no dia a dia uma vez que é esta que dá suporte aos processos.

  A dependência da tecnologia tornou-se tão forte que a indisponibilidade desses sistemas equivale ao impacto da indisponibilidade da própria informação.

  Esta dependência gerou um paradoxo, a mesma tecnologia que permite um acesso cada vez mais simples à informação, também o torna cada vez mais perigoso. A preocupação com a proteção da informação cresce à mesma velocidade que aparecem novas tecnologias, porque uma nova facilidade pode significar uma nova fragilidade.

  O principal desafio deste pilar é encontrar o equilíbrio entre a facilidade de uso, a performance das aplicações e a segurança necessária.

Caso não exista equilíbrio entre os três pilares, a estrutura perde estabilidade, afetando diretamente a Segurança da Informação.

Côrte (2014, p. 90) refere que**:**

> Cada um dos pilares tem a sua importância especifica, porém como eles são interdependentes é necessário que se tenha uma visão integrada sobre eles. A

Segurança da Informação não pode ser suportada isoladamente por um pilar, por mais importante que seja esse pilar, mas solidariamente pelos três."

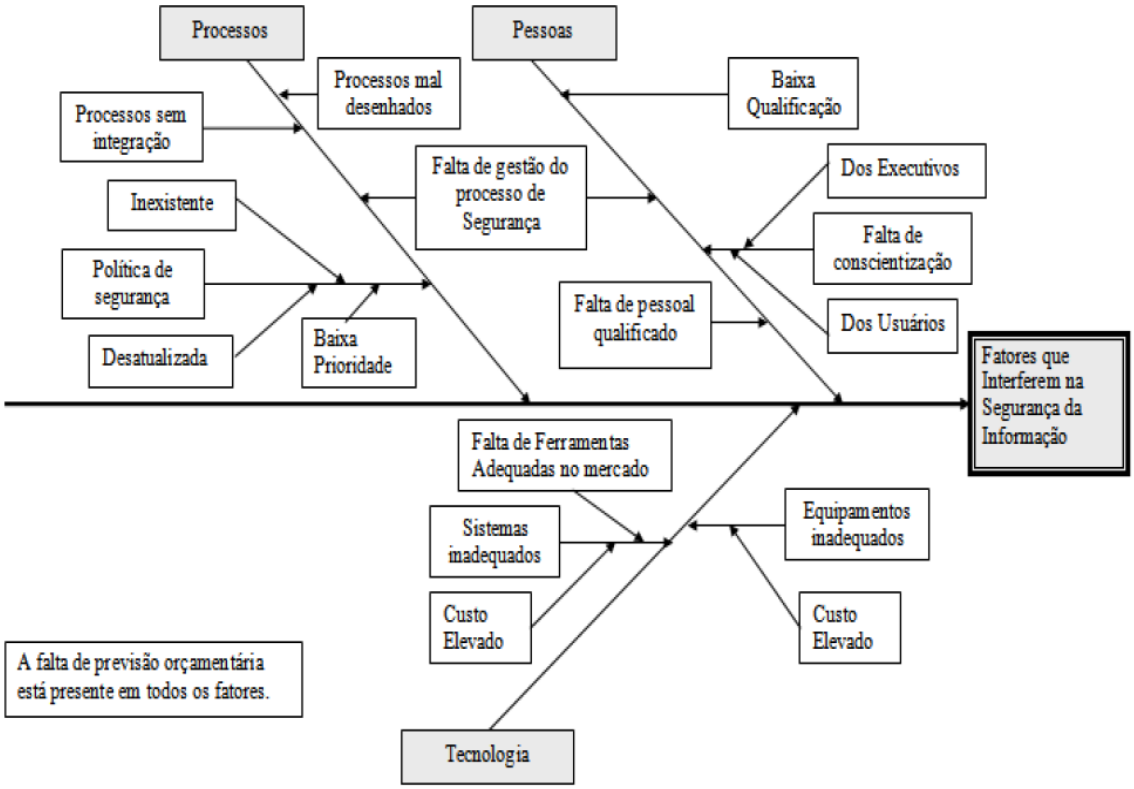

Figura 8: Diagrama de Ishikawa: fatores que interferem na Segurança da Informação (Silva, 2010, p. 55)

Na figura 8, Neto, Martins, Côrte e Silva (2008), citado por Silva (2010) representam através de um diagrama de Ishikawa, os fatores que interferem na Segurança da Informação.

Também Neto, Martins, Côrte e Silva (2008) consideram que Pessoas, Processos e Tecnologia são os três pilares da Segurança da Informação, apresentando para cada pilar um conjunto de fatores a ter em conta para alcançar o sucesso da Segurança da Informação.

2.3.1 Ameaças à Segurança da Informação

Compreender o ciclo de vida da informação (2.1.2) é de suma importância para a Segurança da Informação, pois durante esse ciclo existem condições que, de alguma

forma, a colocam em situação vulnerável, podendo comprometer ativos e processos de trabalho da organização.

De acordo com Sêmola (2014) as condições que afetam a informação são as ameaças, as vulnerabilidade e os riscos:

- **Ameaças:** são agentes ou condições que podem causar incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade da informação;

  Sêmola (2014) classifica as ameaças quanto à sua intencionalidade:

  Naturais: ameaças decorrentes de fenómenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, maremotos, aquecimento, poluição, etc.

  Involuntárias: ameaças inconscientes, quase sempre causadas pelo desconhecimento, podem ser causadas por acidentes, erros, falha de energia etc.

  Voluntárias: ameaças propositadas causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

- **Vulnerabilidades:** são fragilidades existentes ou associadas a ativos que manipulam ou processam informações que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da Segurança da Informação: confidencialidade, integridade e disponibilidade.

  No entanto Sêmola (2014) refere que as vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando de um agente causador ou condição favorável, que são as ameaças, exemplificando alguns tipos de vulnerabilidades:

  Físicas: instalações prediais que não atendem as boas práticas ou as normas e regulamentações vigentes.

  Naturais: ambientes com equipamentos eletrónicos próximos a locais suscetíveis a desastres naturais, como incêndios, enchentes, aumento de humidade, entre outros.

Hardware: equioamentos informáticos são suscetíveis a poeira, humidade, sujeira e acesso indevido a recursos inadequadamente protegidos, podendo ainda sofrer com componentes deficientes ou mal configurados.

Software: Erros na codificação, instalação ou configuração de sistemas e aplicações podem acarretar acessos indevidos, divulgação de informações ou até mesmo indisponibilidade do recurso quando necessário.

Comunicação: as comunicações são vulneráveis a escutas (acesso indevido) ou a problemas na infraestrutura física ou lógica que a impeçam de ser estabelecida.

Humanas: falta de treino ou de consciencialização das pessoas, falta de avaliação psicológica adequada para verificação de antecedentes (*background check*) que identifique objetivos escusos ou problemas anteriores, ou mesmo má fé ou descontentamento de um colaborador.

- **Riscos:** são as probabilidades de ameaças explorarem vulnerabilidades, provocando perdas ou danos aos ativos e às informações. Para neutralizar ou mitigar essa tríade (ameaça-vulnerabilidade-risco) é preciso estabelecer formas estruturadas de proteção que garantam a Segurança da Informação durante todo o seu ciclo de vida e nas diversas camadas ou aspectos em que a mesma é processada ou tratada.

  De acordo com Sêmola (2014, p. 48):

  > risco é a probabilidade de que agentes, que são as ameaças, explorarem vulnerabilidades, expondo os ativos a perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios. Esses impactos são limitados por medidas de segurança que protegem os ativos, impedindo que as ameaças explorem as vulnerabilidades, diminuindo, assim o risco, Sêmola.

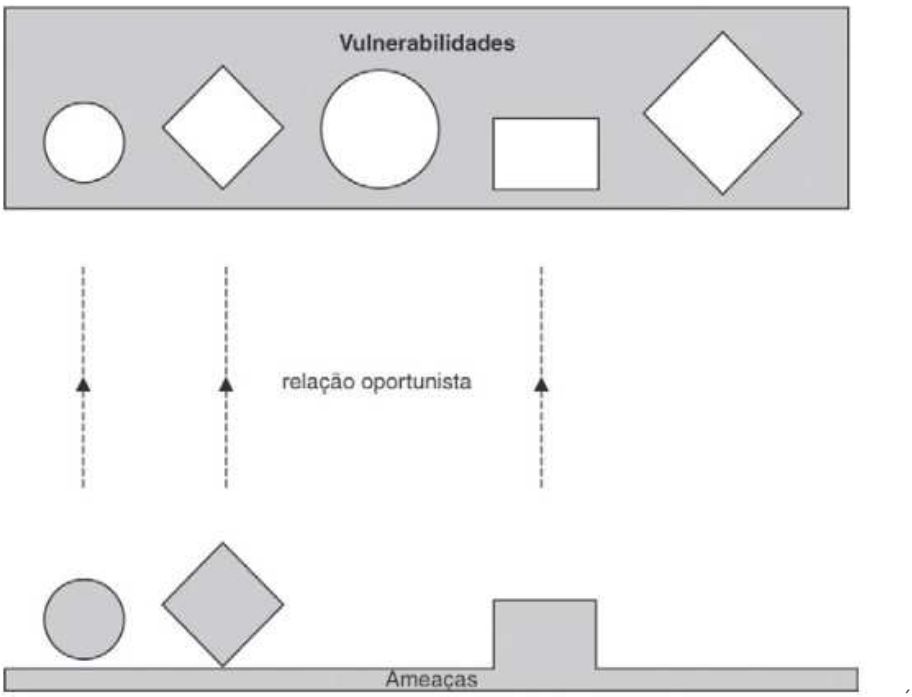

Figura 9: As ameaças específicas exploram vulnerabilidades compatíveis, como peças que encaixam (Sêmola, 2014, p. 19)

Por sua vez, ataque, é o meio que um indivíduo mal-intencionado utiliza para conseguir acesso não autorizado a um Sistema de Informação. Através desse acesso, poderá copiar, apagar ou alterar qualquer informação, no final irá tentar ocultar os vestígios, dificultando assim a perceção do que foi realizado com o ataque.

Para Pinheiro (2007, p. 12):

> Um ataque ocorre quando uma ameaça intencional é realizada. Os ataques ocorrem por motivos diversos. Variam desde a pura curiosidade, passando pelo interesse em adquirir maior conhecimento sobre os sistemas, até ao extremo, envolvendo ganhos financeiros, extorsão, chantagem de algum tipo, espionagem industrial, venda de informações confidenciais e, o que está muito na moda, ferir a imagem de um governo ou de uma determinada empresa ou serviço. Quando isto acontece, a notícia da invasão é proporcional à fama de quem a sofreu e normalmente representa um desastre em termos de repercussão pública.

Para Wadlow (2000) um ataque pode ser classificado como:

- **Ativo**, quando visa a alteração da informação (ou dados);
- **Passivo**, quando visa disponibilizar, roubar informação (ou dados);
- **Destrutivo**, quando visa à negação do acesso a informação (ou dados) ou serviços.

Laureano (2005) classifica as formas possíveis de ataques em sistemas:

- **Intercetação**: acesso a informações por entidades não autorizadas (violação da privacidade e confidencialidade das informações);
- **Interrupção**: pode ser definida como a interrupção do fluxo normal das mensagens ao destino;
- **Modificação**: consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem;
- **Personificação**: ocorre quando uma entidade tenta assumir o papel de outra, ou seja, quando um utilizador não autorizado se faz passar um utilizador autorizado para conseguir ter acesso à informação.

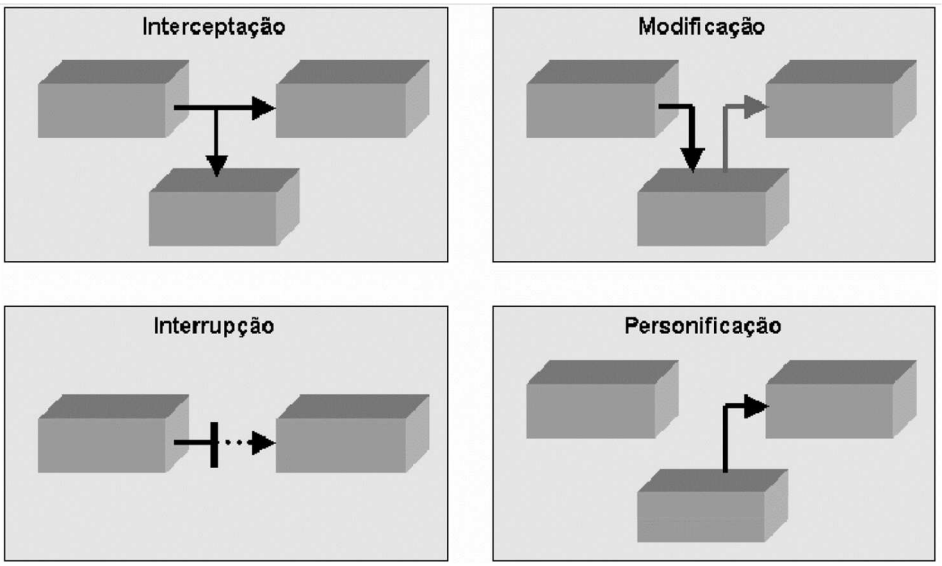

Figura 10: Possíveis formas de ataque a sistemas (Laureano, 2005, p. 17)

Beal (2008) relaciona todos os termos associados ao risco para a Segurança da Informação conforme figura 11:

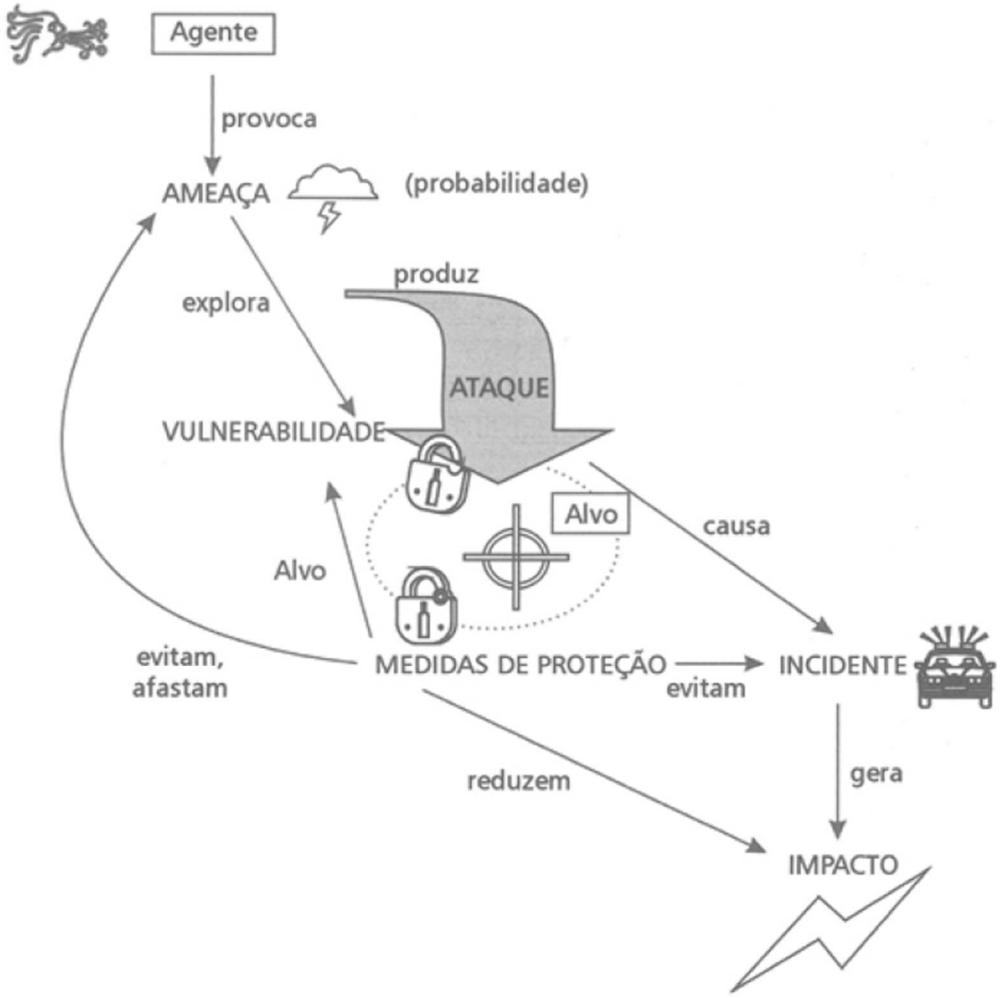

Figura 11: Relação entre os termos associados ao risco para a Segurança da Informação (Beal, 2008, p. 16)

Para Beal (2008) o alvo de um ataque pode ser um ativo de informação. Nesse contexto, a ameaça é um elemento de risco ao qual se pode associar uma probabilidade que por sua vez é calculada a partir da frequência de ocorrência. As medidas de proteção podem reduzir a probabilidade de concretização de uma ameaça e as vulnerabilidades com potencial de exploração, consequentemente corroboram para a redução do risco do ativo de informação.

2.3.2 A Segurança da Informação na Administração Pública Local

Com o aumento da dependência em relação às tecnologias de informação também a Administração Pública Local se deparara com um conjunto de questões que, até ao momento, não se colocavam e que devem ser agora consideradas, tais como:

- Definição e implementação de uma adequada Política de Segurança da Informação, que abarque todo o ciclo de vida da informação, sempre focada na preservação e na segurança, de forma a garantir a produção, armazenamento, uso e disponibilização de informação que cumpra os atributos de autenticidade, integridade, inteligibilidade e de preservação no longo prazo;

- Necessidade de assegurar a privacidade e confidencialidade dos dados pessoais dos munícipes, fornecedores e funcionários;

- Necessidade de salvaguardar os seus ativos (informação) protegendo-se da excessiva dependência dos fornecedores externos de tecnologia;

- Medir a avaliar periodicamente as Políticas de Segurança da Informação de forma fácil e transparente, permitindo retirar ensinamentos que conduzam a melhorias e a um estado de maturidade mais avançado.

Carneiro (2002) refere que é necessária a aplicação de diferentes mecanismos de proteção, deteção e reação, bem como a formulação de políticas de segurança que contribuam para a preservação da confidencialidade, integridade e disponibilidade da informação.

Gouveia e Ranito (2004, p. 91) referem que:

> No caso das autarquias, a pressão é ainda maior, uma vez que tratam com dados muito sensíveis, oficiais e estão num processo de abrir comunicações eletrónicas com o cidadão/munícipe, criando portas de entrada potencialmente perigosas, se não forem devidamente acauteladas.

De acordo com Lopes (2012, p. 1):

> No caso particular das autarquias, onde a informação pública e pessoal deve ser protegida pelos responsáveis, deve haver a preocupação de entender a segurança

> como algo a considerar, logo desde o início, nas atividades de planeamento e desenvolvimento de SI.

A mesma autora salienta ainda que:

> os munícipes esperam das autarquias o desenvolvimento e modernização dos seus Sistemas de Informação (SI), com vista à disponibilização de serviços que melhorem o seu bem-estar e a sua qualidade de vida. Para a satisfação deste propósito, defende-se que as tecnologias e sistemas utilizados têm de transmitir confiança aos munícipes, pelo que se torna necessário considerar aspetos relacionados com a Segurança da Informação e dos sistemas e tecnologias que manipulam essa informação (Lopes, 2012, p. vii).

Para obter esta confiança por parte dos munícipes é necessário garantir a existência de segurança nos portais de acesso, a proteção das redes de transmissão e tecnologias de suporte à informação e comunicação e, a confidencialidade das bases de dados.

Sobre a temática de segurança das Tecnologias de Informação e Comunicação na Administração Pública Local existe um estudo, denominado Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Câmaras Municipais (IUTICCM), que é realizado anualmente pela Direção-Geral de Estatísticas da Educação e da Ciência (DGEEC) em conjunto com a Direção de Serviços de Estatísticas da Ciência e Tecnologia e da Sociedade de Informação (DSECTSI).

Este inquérito é realizado *on-line*, junto das Câmaras Municipais do continente e regiões autónomas, num universo de 308, com uma taxa de resposta de 100%.

Encontram-se disponíveis, desde outubro, os dados referentes a 2019, repartidos por várias publicações, das quais destacamos:

- Segurança das TIC (cibersegurança) na Administração Pública Central, Regional e Câmaras municipais (DGEEC & DSECTSI, 2020a);
- Transformação Digital na Administração Pública Central, Regional e Câmaras Municipais (DGEEC & DSECTSI, 2020b).

Nestes relatórios são apresentados alguns dos indicadores mais relevantes das operações de inquirição relativas a 2019 de onde realçamos:

Na tabela 1 é possível verificar que 67% dos municípios nacionais têm uma estratégia de Segurança da Informação definida, sendo que destes, apenas 26% já a têm em concordância com o Regulamento Geral sobre a Proteção de Dados (RGPD).

	2019	
	Nº	%
Câmaras Municipais que têm definida uma estratégia para a segurança de informação	205	67
Nível de concordância face ao RGPD :		
Já se encontra de acordo com o RGPD	54	26
Encontra-se em fase de revisão de modo a incorporar o RGPD	140	68
Não se encontra em conformidade com o RGPD	11	5

Tabela 1: Câmaras Municipais que têm definida uma estratégia para a segurança de informação e o nível de concordância face ao RGPD
(DGEEC & DSECTSI, 2020a; DGEEC & DSECTSI, 2020b)

No entanto, de acordo com a tabela 2, quando questionados sobre se possuem recomendações sobre medidas, práticas ou procedimentos de segurança das Tecnologias de Informação e Comunicação por tipo de assunto, apenas 36% dos municípios indicam possuir.

	2019	
	Nº	%
Câmaras Municipais que possuem recomendações sobre medidas, práticas ou procedimentos de segurança das TIC	111	36
Assuntos considerados nessas recomendações:		
Gestão dos níveis de acesso às TIC	102	92
Responsabilidade, direitos e deveres no que respeita à utilização das TIC	99	89
Armazenamento, proteção, acesso e processamento de dados	98	88
Procedimentos ou regras para prevenir ou reagir a incidentes de segurança	83	75
Formação do pessoal ao serviço para uma utilização segura das TIC	62	56
Período em que foram definidas ou revistas essas recomendações:		
Nos últimos 12 meses	68	61
Há mais de 12 meses e até 24 meses	21	19
Há mais de 24 meses	22	20

Tabela 2: Câmaras Municipais que possuem recomendações sobre medidas, práticas ou procedimentos de segurança das TIC por tipo de assunto considerado nas mesmas
(DGEEC & DSECTSI, 2020a)

Na tabela 3 é possível verificar que a única medida de segurança implementada pela totalidade dos municípios é a atualização do software, que 50% fazem testes de segurança

às Tecnologias de Informação e Comunicação e que apenas 42% faz a identificação e autenticação do utilizador através de métodos biométricos.

	2019	
	Nº	%
Atualização regular do software	307	100
Controlo de acessos à rede do Organismo	286	93
Autenticação dos utilizadores através de uma palavra passe segura	262	85
Conservação de registos para análise após a ocorrência de incidentes	209	68
Testes da segurança às TIC	154	50
Técnicas de encriptação de dados, documentos ou e-mails	151	49
Avaliação dos riscos ligados às TIC	144	47
Identificação e autenticação do utilizador através de métodos biométricos	128	42

Tabela 3: Tipo de medidas de segurança das TIC implementadas nas Câmaras Municipais (DGEEC & DSECTSI, 2020a)

Na tabela 4 verifica-se que, em 2019, 15% dos municípios detetaram problemas de segurança informática relacionados com as Tecnologias de Informação, sendo que a principal causa foram ataques externos que deixaram indisponíveis os serviços de Tecnologias de Informação e Comunicação.

	2019	
	Nº	%
Câmaras Municipais que detetaram problemas de segurança informática	47	15
Problemas devido a incidentes de segurança relacionados com as TIC:		
Indisponibilidade de serviços TIC, devido a ataques externos	29	62
Destruição ou corrupção de dados devido a ataque ou incidentes inesperados	22	47
Divulgação de dados confidenciais, devido a ataques de intrusão (ex. *pharming* ou *phishing*)	8	17
Outros	4	9

Tabela 4: Câmaras Municipais que indicaram ter detetado problemas de segurança informática por tipo de incidentes de segurança relacionados com as TIC. (DGEEC & DSECTSI, 2020a)

21% dos municípios possuem seguro contra incidentes de seguranças das Tecnologias de Informação e Comunicação de acordo com a tabela 5.

	2019	
	Nº	%
Câmaras Municipais que têm seguro contra incidentes de segurança das TIC	21	7

Tabela 5: Câmaras Municipais com seguro contra incidentes de segurança das TIC (DGEEC & DSECTSI, 2020a).

A tabela 6 demonstra que existe um elevado número de municípios que sentem uma grande necessidade de reforçar as competências em segurança das Tecnologias da Informação e Comunicação, sendo que se destacam as áreas de segurança e de privacidade de dados

	2019	
	Nº	%
Câmaras Municipais com elevada necessidade de reforço de competências em segurança das TIC, por tipo de competência:		
Segurança	139	45
Privacidade dos dados	128	42
Gestão de infraestruturas	61	20
Testes e certificação	61	20
Data Science	51	17
Gestão de projeto	45	15
Manutenção aplicacional	42	14
Desenvolvimento de novas aplicações	38	12
Suporte aos utilizadores (helpdesk)	38	12
Definição da arquitetura empresarial	32	10
Gestão da relação com o negócio	21	7

Tabela 6: Câmaras Municipais que indicaram, com grau elevado, a necessidade de reforçar as competências TIC, por tipo de competência. (DGEEC & DSECTSI, 2020b).

Na tabela 7 é possível observar a evolução do número de problemas de Segurança Informática e o tipo de incidente detetados pelos municípios nos últimos três anos.

Apesar de não se conseguir identificar um padrão de evolução no número de ocorrências verifica-se que a indisponibilidade de serviços de Tecnologia de Informação e Comunicação devido a ataques externo é o incidente que vem, tendencialmente, aumentando nos últimos três anos.

Unidade: %

	2017	2018	2019
Câmaras Municipais que detetaram problemas de segurança informática	19	11	15
Problemas devidos a este tipo de incidentes :			
Destruição ou corrupção de dados devido a ataque ou incidentes inesperados	70	55	47
Indisponibilidade de serviços TIC, devido a ataques externos	26	33	62
Outros	18	24	9
Divulgação de dados confidenciais, devido a ataques de intrusão (ex. *pharming* ou *phishing)*	4	3	17

Tabela 7: Câmaras Municipais que detetaram problemas de segurança entre 2017-2019. (DGEEC & DSECTSI, 2020a) e (DGEEC & DSECTSI, 2019).

De forma resumida, apesar da importância que a Informação e os Sistemas de Informação assumem atualmente, apenas 67% das Câmara Municipais tem definida uma estratégia para a Segurança da Informação e destas, somente, 6% se encontra de acordo com o RGPD (Regulamento Geral da Proteção de Dados). Unicamente 36% dos Municípios possuem recomendações sobre medidas, práticas ou procedimentos, elemento essencial para que cada pessoa compreenda o que precisa de fazer e quando precisa de fazer.

Apesar de 15% dos Municípios, em 2019, terem detetado problemas de Segurança da Informação, principalmente devido a ataques externos que deixaram os serviços de Tecnologia de Informação e Comunicação indisponíveis (62%), apenas 50% fazem testes de Segurança das de Tecnologia de Informação e Comunicação, 47% avaliam os riscos ligados às de Tecnologia de Informação e Comunicação e 7% possuem seguro contra incidentes de segurança das de Tecnologia de Informação e Comunicação.

Face ao exposto, uma grande parte dos Municípios sente necessidade de reforçar as competências em Segurança das de Tecnologia de Informação e Comunicação, principalmente ao nível da segurança (45%) e da privacidade dos dados (42%).

Os dados apresentados, referentes a 2019, demonstram a necessidade de se efetuar uma avaliação aos Sistemas de Informações dos Municípios, de forma a conhecer a realidade e a introduzir melhorias de forma a alcançar um estado de maturidade mais avançado.

2.4 Principais *Standards*/Normas de Segurança da Informação

> Os computadores e os ambientes em que estes operam são dinâmicos. A tecnologia e os utilizadores do sistema, os dados e a informação nos sistemas, os riscos associados ao sistema e, portanto, os requisitos de segurança estão em constante mudança. Muitos tipos de alterações afetam a segurança do sistema: desenvolvimentos tecnológicos (quer adotados pelo proprietário do sistema ou disponíveis para utilização por outros), ligação a redes externas, uma mudança no valor ou utilização da informação, ou o surgimento de uma nova ameaça.
>
> Além disso, a segurança nunca é perfeita quando um sistema é implementado. Os utilizadores e operadores do sistema descobrem novas formas de contornar ou subverter intencionalmente a segurança. Alterações no sistema ou no ambiente podem criar novas vulnerabilidades. A adesão estrita aos procedimentos é rara, e os procedimentos tornam-se desatualizados com o tempo. Todas estas questões tornam necessária uma reavaliação da segurança dos sistemas informáticos. (Guttman & Roback, 1995, p. 13 e 14, tradução própria).

Proteger a informação é um desafio que requer procedimentos, estratégias e diretrizes que devem ser seguidos, sendo necessário cumprir com as melhores práticas aceites e reconhecidas internacionalmente.

As normas técnicas de boas práticas ou *standards* relacionados com a Segurança da Informação têm vindo a evoluir de forma a acompanhar a nova realidade dos Sistemas de Informação.

Estes *standards* / normas são desenvolvidos por entidades que são uma referência a nível mundial, consubstanciam a visão e concordância de intervenientes importantes sobre as melhores praticas a adotar e os controlos recomendados a implementar. Têm como objetivo orientar as atividades realizadas com o objetivo de tornar os Sistemas de Informação mais seguros.

As normas e *standards*, mais amplamente adotadas em todo, na área de Segurança da Informação o mundo são, nomeadamente:

- COBIT - *Control Objectives for Information and Related Technology*;
- ITIL - *Information Technology Infrastructure Library*;

- ISO/IEC 27002:2013 - *Information Technology — Security Techniques — Code of Practice for Information Security Controls*.

Não sendo praticável, no âmbito deste projeto, o aprofundamento de todos as normas e *standards* de segurança, foi efetuada uma comparação entre as diversas metodologias de forma a identificar a que mais se adequava ao objetivo pretendido, concluindo-se que as orientações da norma ISO/IEC 27002:2013 são as que mais se ajustam.

De forma sucinta a metodologia **COBIT** é uma *framework* integradora de processos de governança e gestão das Tecnologias de Informação, que ajuda as organizações a desenvolver, organizar e implementar estratégias em torno da gestão da informação e governança, alinhando as metas de Tecnologia de Informação com as metas do negócio.

Ou seja, mesmo contendo indicadores relacionados com a segurança de Sistemas de Informação, esta abordagem está mais focada no negócio e na gestão da informação de uma forma generalizada, o que poderia levar a uma visão subdimensionada dos riscos, objetivos de controlo e controlos específicos para a Segurança da Informação, que se encontram mais apropriadamente especificados na ISO/IEC 27002:2013.

Por sua vez a metodologia **ITIL** é uma *framework* para gerir os serviços de Tecnologias de Informação, mais orientada para ser utilizada na definição de estratégias e processos de operações relacionados com Tecnologias de Informação. É um conjunto estruturado de boas práticas em que os vários processos comunicam entre si, cada com o seu papel para que, no final, possam dar resposta a duas questões: a melhoria contínua e a satisfação do cliente, o seu principal objetivo é a melhoria da qualidade dos serviços de Tecnologia da Informação, com foco no cliente.

Apesar de contemplar processos relacionados com a segurança de TI, nomeadamente, processos de suporte aos serviços (gestão de incidentes, gestão de problemas, gestão da configuração, gestão de mudanças e gestão de liberação) e de entrega de serviços (gestão da capacidade, gestão da disponibilidade e gestão da continuidade dos serviços de TI), a gestão da Segurança da Informação envolve muitas outras disciplinas, e não poderia ser suportada apenas na análise destes controlos e processos de Tecnologia de Informação, razão pela qual o ITIL não se revelou a ferramenta adequada para este trabalho.

A escolha da norma ISO/IEC 27002:2013 deveu-se ao facto de esta ser considerada, a nível mundial, “o padrão” para a gestão da Segurança da Informação, foi desenvolvida

especificamente para estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de Segurança da Informação, podendo ser utilizada em qualquer tipo de organização, pública ou privada, de pequeno ou grande porte, com ou sem fins lucrativos, e não apenas em empresas de tecnologia.

"Trata-se, no fundo, de um código de boas práticas que inclui um extenso conjunto de controlos que indicam a forma de atuação para que os objetivos definidos nas políticas possam ser atingidos" (Carvalho, 2018, p. 18).

O facto de ser integralmente fundamentada na Segurança da Informação torna-a a solução mais completa e abrangente, a sua amplitude e facilidade de aplicação tornaram esta norma não apenas alvo de destaque, mas a primeira escolha para uma análise mais aprofundada.

2.4.1 ISO/IEC 27002:2013

As normas da família ISO 27000 também conhecidas como série ISO 27000, foram publicadas pelas organizações internacionais ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), integram todas as características que os peritos na área consideraram importantes (razão pela qual é uma norma de padrão internacional) e explicam como aplicar as melhores práticas de Segurança da Informação na implementação de um sistema de gestão de Segurança da Informação (SGSI).

Uma das normas desta série é a ISO/IEC 27002:2013, onde se define um código de boas práticas para a gestão de Segurança da Informação, podendo ser utilizada para apoiar a implementação do um Sistema de Gestão de Segurança da Informação (SGSI) em qualquer tipo de organização, pública ou privada, de pequeno ou grande porte, com ou sem fins lucrativos.

Esta norma tem como objetivo fornecer diretrizes para práticas de gestão de Segurança da Informação e normas de Segurança da Informação para as organizações, incluindo a seleção, a implementação e gestão de controlos, levando em consideração os ambientes de risco da Segurança da Informação da organização (ISO/IEC 27002:2013, 2013).

A norma está estruturada em 19 secções, 14 das quais sobre Segurança da Informação, 35 objetivos de controlo e 114 controlos.

As 14 secções sobre Segurança da Informação, abrangem a Segurança da Informação em todos os seus aspetos, tratando de ferramentas, processos e pessoas, envolvendo soluções tecnológicas, documentação de processos e consciencialização de pessoas.

A ordem em que se encontram as secções não indicam o seu significado nem o seu grau de importância, da mesma forma os controlos não estão por ordem de prioridade, a sua relevância é determinada pelo risco especifico a que cada organização está exposta.

Os capítulos 0 a 4 são a introdução da norma, os capítulos a partir do 5 são sobre Segurança da Informação.

De forma a demonstrar a abrangência da norma, são apresentadas abaixo, de forma sucinta, as 19 secções da norma:

0: Introdução - Faz o enquadramento histórico, explica o objetivo da ISO/IEC 27002:2013 e a sua compatibilidade com outras normas.

1: Objetivo - Apresenta os objetivos que a norma pretende alcançar.

2: Referência Normativa - Refere a ISO/IEC 27000 como a norma de referência.

3: Termos e Definições - Refere a ISO/IEC 27000 como a norma onde os termos e definições são dados.

4: Estrutura desta Norma - Apresenta a forma como a norma se encontra estruturada.

5: Políticas de Segurança da Informação – Indica como deve ser criado o documento sobre a política de Segurança da Informação da empresa, os principais conceitos que deve conter, a definição das estruturas que irão identificar os objetivos e modos de controlo, o comprometimento da direção com a política, entre outros fatores.

6: Organização da Segurança da Informação - Para implementar a Segurança da Informação numa organização, é necessário estabelecer uma estrutura para geri-la de forma adequada. Para isso, as atividades de Segurança da Informação devem ser coordenadas por representantes da organização, que devem ter as suas responsabilidades bem definidas e proteger as informações de caráter sigiloso.

7: Segurança em Recursos Humanos – Refere que antes da contratação de um funcionário ou fornecedor, é importante que cada um deles entenda as suas responsabilidades e concorde com o papel que irá desempenhar. Quaisquer candidatos devem ser devidamente analisados, principalmente se forem lidar com informações de caráter sigiloso. A intenção é mitigar o risco de roubo, fraude ou mau uso dos recursos.

8: Gestão de Ativos - De acordo com a norma, ativo é tudo aquilo que tem valor para a empresa, devendo ser devidamente protegido. Para isso, os ativos devem ser identificados e classificados de forma a que se possa estruturar um inventário de ativos e mante-lo atualizado. Também deve de existir um documento com regras bem definidas sobre o uso desses ativos, e sobre as responsabilidades de proteção dos mesmos.

9: Controlo de Acessos – Indica que o acesso à informação, aos recursos de processamento das informações e aos processos de negócios, deve ser controlado. Assim, deve ser assegurado o acesso aos utilizadores autorizados (principio da disponibilidade) e prevenido o acesso não autorizado a Sistemas de Informação, (garantindo a confidencialidade da informação), de forma a evitar danos em documentos e recursos de processamento da informação.

10: Criptografia – Refere que a criptografia deve ser utilizada para proteger a confidencialidade, autenticidade e/ou integridade da informação. Neste sentido deve ser desenvolvida e implementada uma política para o uso de controlos criptográficos, esta política deve incluir os requisitos para a gestão das chaves criptográficas ao longo de todo o seu ciclo de vida incluindo, geração, armazenagem, arquivo, recuperação, distribuição retirada e destruição das chaves.

11: Segurança Física e do Ambiente – Menciona que as instalações de processamento de informação e as informações criticas ou sensíveis devem ser mantidas em segurança, com níveis e controles de acesso apropriados, incluindo proteção física. Essa proteção deve ser compatível com os riscos previamente identificados.

Os equipamentos também devem ser protegidos contra ameaças físicas e ambientais, incluindo aqueles utilizados fora do local.

12: Segurança nas Operações – Refere que deve ser garantida a operação segura e correta dos recursos de processamento da informação.

São necessários controles de *malware*, a instalação de *software* deve ser controlada e as vulnerabilidades técnicas devem ser corrigidas.

Os procedimentos de operação devem ser documentados e disponibilizados a todos os utilizadores que deles necessitem.

Devem ser efetuados *backups* (cópias de segurança) e mantidos de acordo com uma política de *backup*.

Todas as atividades do utilizador e do administrador devem ser registadas, gerar evidências e ser protegidos, os relógios devem estar sincronizados.

13: Segurança nas Comunicações – Nesta secção é referida a forma como deve ser garantida a proteção das informações em redes e dos recursos de processamento da informação que os apoiam.

14: Aquisição, Desenvolvimento e Manutenção de Sistemas – Refere que deve ser garantido que a Segurança da Informação é parte integrante de todo o ciclo de vida dos Sistemas de Informação e que está projetada e implementada no desenvolvimento do ciclo de vida dos Sistemas de Informação. Também deve ser tido em conta que os dados utilizados em testes devem ser selecionados com cuidado, protegidos e controlados.

15: Relacionamento com Fornecedores – O objetivo desta secção é garantir a proteção dos ativos da organização que estão acessíveis aos fornecedores. Deve ser mantido um nível acordado de Segurança da Informação e de entrega de serviços em consonância com o acordado com os fornecedores.

Refere ainda que o serviço executado por fornecedores deve ser monitorizado, analisado criticamente e auditado regularmente. As mudanças de serviços devem ser controladas.

16: Gestão de Incidentes de Segurança da Informação – Esta secção refere que deve ser assegurado um enfoque consistente e efetivo para gerir os incidentes de Segurança da Informação, incluindo a comunicação sobre fragilidades e eventos de Segurança da Informação, para que estes sejam corrigidos rapidamente.

17: Aspetos da Segurança da Informação na Gestão da Continuidade do Negócio – Refere que a continuidade da Segurança da Informação deve ser planeada, implementada e revista como parte integrante dos sistemas de gestão de continuidade de negócios da organização.

O objetivo é impedir a interrupção das atividades e garantir que as operações essências são recuperadas no mais curto espaço de tempo.

18: Conformidade – Este secção refere que a organização deve identificar e documentar as suas obrigações com as autoridades externas e outros terceiros em relação à Segurança da Informação, incluindo propriedade intelectual, proteção de registos, privacidade / informações de identificação pessoal e criptografia, de forma a evitar a violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas com a Segurança da Informação e de quaisquer requisitos de segurança.

Cada uma das secções apresentadas tem uma ou mais categorias de controlo. Cada categoria de controlo contém um objetivo de controlo, onde é indicado o que se espera alcançar e um ou mais controlos que devem ser aplicados para alcançar o objetivo de controlo.

Cada controlo tem definido o que deve ser feito para atingir o objetivo de controlo, havendo ainda diretrizes de implementação onde são apresentadas informações detalhadas para apoiar a implementação do controlo e alcançar o objetivo de controlo.

Vejamos por exemplo as diretrizes de implementação do controlo 5.1.1:

5. Política de segurança - Secção de Controlo da Segurança da Informação

5.1 Política de Segurança da Informação - Categoria de Controlo

> Fornecer uma orientação e apoio da gestão para a Segurança da Informação de acordo com os requisitos do negócio e com as leis e regulamentos aplicáveis**. -** Objetivo de Controlo

5.1.1 Documento da política Segurança da Informação - Controlo

> Um documento de política de Segurança da Informação deve ser aprovado pela gestão, publicado e comunicado a todos os empregados e partes externas relevantes.
>
> Diretrizes para implementação:

É necessário que o mais alto nível da organização defina uma política de Segurança da Informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerir os objetivos de Segurança da Informação.

Convém que as políticas de Segurança da Informação contemplem requisitos oriundos da:

a) estratégia do negócio;
b) de regulamentações, legislação e contratos;
c) do ambiente de ameaça da Segurança da Informação, atual e futuro.

É necessário que a política de Segurança da Informação contenha declarações relativas a:

a) definição da Segurança da Informação, objetivos e princípios para orientar todas as atividades relativas à Segurança da Informação;
b) atribuição de responsabilidades, gerais e específicas na gestão da Segurança da Informação para os papéis definidos;
c) processos para o tratamento dos desvios e exceções.

Ao nível mais baixo da organização, convém que a política de Segurança da Informação seja apoiada por políticas de tópicos específicos, que exijam a implementação de controlos de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos.

São exemplos de políticas com tópicos específicos:

a) controlo de acesso (A.9);
b) classificação e tratamento da informação (A.8.2);
c) segurança física e do ambiente (A.11);
d) tópicos orientados aos usuários finais:
    1) uso aceitável dos ativos (A.8.1.3);
    2) mesa limpa e ecrã limpo (A.11.2.9);
    3) transferência de informações (A.13.2.1);
    4) dispositivos móveis e trabalho remoto (A.6.2);
    5) restrições sobre o uso e instalação de software (A.12.6.2);
e) *backup* (A.12.3);
f) transferência da informação (A.13.2);
g) proteção contra vírus (*malware*) (A.12.2);

h) gestão de vulnerabilidades técnicas (A.12.6.1);
i) controlos criptográficos (A.10);
j) segurança nas comunicações (A.13);
k) proteção e privacidade da informação de identificação pessoal (ver 18.1.4);
l) relação com fornecedores (ver 15).

2.5 Modelo de Maturidade

Um modelo de maturidade é uma ferramenta de auditoria e de medição de performance que permite medir o progresso face a objetivos definidos.

> Um modelo de maturidade integrado (CMMI) é um modelo de referência que contém práticas (genéricas ou especificas) necessárias à maturidade, em disciplinas especificas como Engenharia de Sistemas, Engenharia de *Software*, Engenharia de *Hardware*, Desenvolvimento Integrado de Produtos, Aquisição e suporte, dando uma visão estruturada da melhoria de processos de uma organização (Lima, 2016).

A utilização de um modelo de maturidade permite identificar lacunas que representam riscos de segurança e pontos de melhoria, é como um guia para avaliar e perceber em que ponto a organização se encontra e orientar melhorias de forma a chegar a um nível de maturidade mais elevado, sempre em busca da excelência.

A utilização destes modelos insere o fator tempo no processo de gestão da Segurança da Informação, o que incute transparência ao processo, permitindo a comparação entre ciclos de avaliação e, até mesmo, entre organizações (*benchmark*).

De acordo com (Trigacheiro, 2012, p. 65 e 66)

> o CMMI (*Capability Maturity Model Integration*) é um modelo de referência que contém práticas (genéricas ou específicas) necessárias à maturidade em disciplinas específicas [*Systems Engineering (SE), Software Engineering (SW), Integrated Product and Process Development (IPPD), Supplier Sourcing (SS)*]. Foi desenvolvido pelo SEI (*Software Engineering Institute*), da Universidade Carnegie Mellon e é uma evolução do CMM, que procura estabelecer um modelo

único para o processo de melhoria corporativo, integrando diferentes modelos e disciplinas.

O mesmo autor refere que:

> Este modelo define seis níveis para medir a maturidade dos processos de TI.
>
> - **0 - Inexistente** – A organização não reconhece a existência de um processo a ser seguido.
> - **1 – Inicial / ad hoc** – O processo de segurança está deficientemente definido. Há evidências de que a organização reconhece que o processo existe, no entanto, os processos não estão normalizados, isto é, são aplicados de forma *ad-hoc* e casuística.
> - **2 – Repetitivo / consistente** – Abordagem repetitiva e disciplinada à realização do processo de segurança. Os processos são desenvolvidos de forma semelhante por pessoas que desenvolvem a mesma tarefa. Não há uma política de formação e comunicação de procedimentos normalizados. Há um alto grau de dependência do conhecimento dos indivíduos e, portanto, os erros são prováveis.
> - **3 – Definido / integrado** – Existem procedimentos para melhorar e aprofundar a segurança dos Sistemas de Informação. Os processos estão normalizados e documentados e são divulgados em formação. É obrigatório que os processos sejam seguidos, pelo que é improvável que sejam detetados desvios. Os processos não são sofisticados, mas existe a formalização das práticas existentes.
> - **4 – Gerido e mensurado** – Os procedimentos de segurança estão interligados e suportam o planeamento estratégico da organização. A gestão faz a monitorização e mensuração da conformidade com os procedimentos e toma medidas quando os procedimentos não atuam efetivamente. Os processos são melhorados frequentemente de acordo com as boas práticas. São usados automatismos e ferramentas de forma limitada e fragmentada.
> - **5 - Otimizado** – Processo de melhoria contínua. Os processos são refinados ao nível das boas práticas, baseados nos resultados de contínuas melhorias e de modelagem de maturidade com outras organizações. As

tecnologias de informação são usadas de forma integrada para automatizar o fluxo de trabalho, fornecendo ferramentas para melhorar a qualidade e eficácia, tornando a organização rápida na adaptação (Trigacheiro, 2012, p. 66).

3 Caracterização da Instituição

O Município de Torres Novas (MTN) agrega 10 freguesias, localiza-se no distrito de Santarém e é habitado por 36.717 (2011) torrejanos numa área total de 270,0 km^2 (cm-torresnovas, 2021).

No seu mapa de pessoal o MTN, para o ano de 2020, contou com 625 lugares, sendo que destes, 540 postos de trabalho estavam efetivamente ocupados no início do ano.

3.1 Divisão de Tecnologias de Informação, Comunicação e Modernização Administrativa (DTICMA)

A DTICMA está dependente da presidência e desenvolve a sua ação nos domínios de:

- aplicações e Sistemas de Informação;
- infraestruturas, suporte e manutenção;
- projetos e desenvolvimento;
- sistemas, redes e comunicação;
- comunicação e imagem.

As Atribuições e Competências da DTICMA no âmbito das áreas de informática e tecnologias de informação estão definidas no Despacho n.º 8175/2020 (2020) (Anexo 1).

3.2 Rede do Município de Torres Novas

Em termos de estrutura física, os edifícios dos diferentes serviços do MTN encontram-se dispersos, localizados em diferentes espaços na cidade (serviços e estabelecimentos de ensino) e freguesias (estabelecimento de ensino).

O centro de dados está localizado num edifício reabilitado e os equipamentos municipais estão ligados ao centro de dados por um sistema de comunicação de dados, utilizando uma infraestrutura maioritariamente em fibra ótica e nalguns locais mais remotos, onde

ainda não foi possível levar a infraestrutura de rede em fibra ótica, as ligações são efetuadas através de radio frequência.

Esta infraestrutura de rede permite a interligação dos diferentes edifícios num sistema de comunicação de dados que suporta a rede local dos computadores (275 computadores), rede local de impressão (60 impressoras), sistema de comunicações de voz (260 telefones), sistema de videovigilância (cerca de 80 câmaras) e ainda a rede de acesso público *Wi-Fi* cujo número de pontos de acesso ascende a cerca de 100 equipamentos.

3.3 Centro de Dados do Município de Torres Novas

O centro de dados do Município de Torres Novas encontra-se numa sala técnica onde estão instalados os circuitos de acesso à Internet, os Core *switches* que interligam os vários edifícios e os servidores aplicacionais da organização.

O Município de Torres Novas dispõe de vários sistemas de virtualização de servidor, o que facilita a gestão do ambiente aplicacional e permite, entre outras funcionalidades, adicionar memória, disco ou aumentar a capacidade de processamento (CPU) nas máquinas virtuais sem perda de serviço, fazer movimentação de servidores virtuais entre servidores físicos, sem *downtime*. Esta infraestrutura conta atualmente com cerca de 50 servidores virtuais.

Este sistema de virtualização está instalado de modo totalmente redundante, o que significa que caso exista uma falha num dos servidores, as máquinas (servidores) virtuais associadas ao mesmo passam a ser executadas utilizando os recursos disponíveis fornecidos pelos outros servidores do cluster.

O sistema de cópias de segurança (*backup*) é feito ao longo do dia para um servidor que está noutra localização. Este servidor aloja as várias cópias de segurança ao longo do dia e ao fim de semana cria uma réplica das cópias de segurança para banda magnética de forma a que possa no início da semana seguinte ser armazenada numa terceira localização segura. Desta forma, seguindo as melhores práticas da indústria, é possível garantir recuperação em situação de catástrofe ou desastre que torne o centro de dados indisponível.

3.4 Ambientes Aplicacionais

O MTN dispõe de várias aplicações que são fundamentais ao bom funcionamento do município e servem de apoio à gestão, o ERP AIRC é composto por um conjunto de módulos, completamente integrados, que abrangem quase a totalidade das áreas de atividade do município, como é possível observar na figura 12.

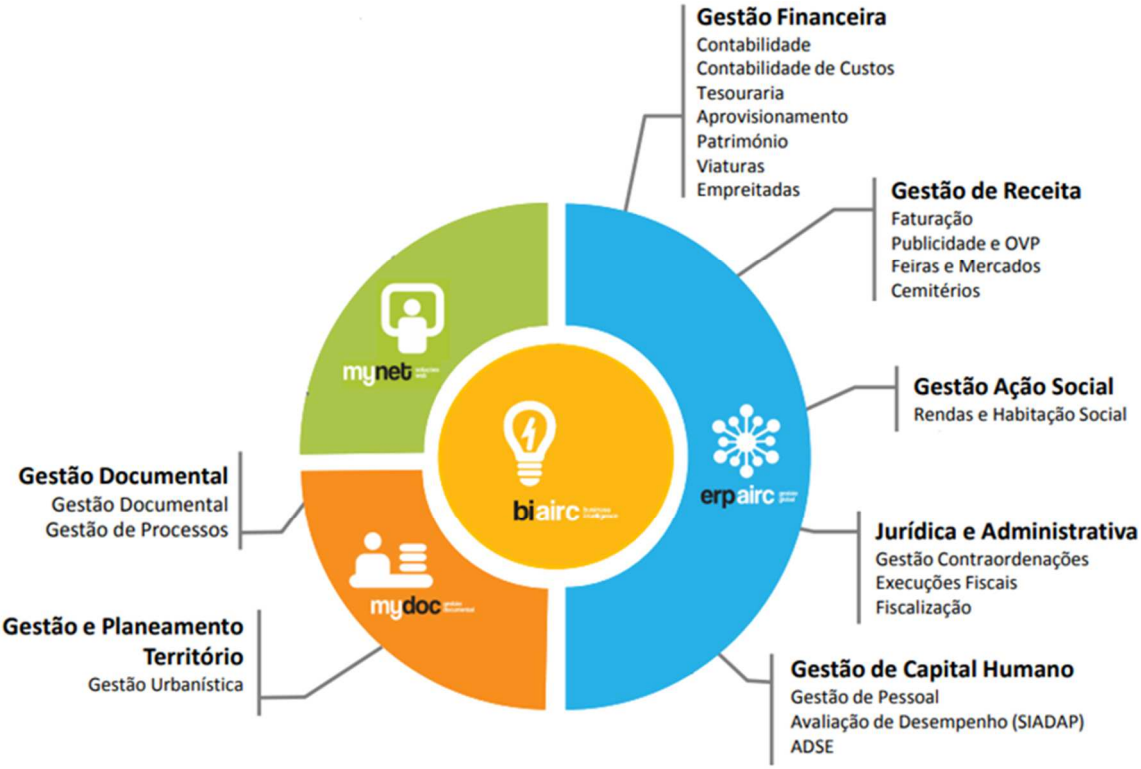

Figura 12: ERP AIRC - Módulos utilizados pelo Município de Torres Novas (Adaptado de: AIRC, s.d.)

Desta integração (lógica e funcional), resulta uma completa unificação de movimentos, baseada na utilização dinâmica de uma única base de dados, que fundamentalmente evita a redundância de processos e de registos (AIRC, 2021).

Para prevenir acessos não autorizados e assegurar o correto uso da informação mantida, o ERP AIRC permite associar os utilizadores a perfis funcionais de utilização e/ou restringir o acesso e utilização a funcionalidades ou categorias de informação (AIRC, 2021).

O perfil de utilizador define o tipo de ações que esse utilizador pode realizar na aplicação, ou seja, são as permissões disponíveis.

De uma forma geral estão identificados quatro tipos de perfil de utilizador para as aplicações: Administrador, Avançado, Utilizador e Consulta. Dentro de cada aplicação as permissões são diferentes e podem haver sub-perfis.

Existem também outras aplicações, desenvolvidas internamente pela DTICMA, que visam colmatar algumas necessidades específicas dos serviços a que o ERP AIRC não dá resposta. Algumas destas aplicações utilizam *Web Services* (solução utilizada na integração de sistemas e na comunicação entre aplicações diferentes), que permitem a utilização de dados do ERP AIRC para a produção de mapas utilizados na área de gestão e/ou criação de outras aplicações.

3.5 Caracterização Informática de um Posto de Trabalho

Um posto de trabalho no Município de Torres Novas é caracterizado, tipicamente, pelo equipamento computador de secretária, telefone IP, pelo software (Microsoft Windows e Office Professional e as necessárias aplicações do ERP AIRC) e ainda por um conjunto de recursos de rede:

- acesso à Internet;
- acesso ao portal de intranet;
- caixa de email pessoal com 5GB;
- caixa(s) de email de serviço partilhada(s) com 5GB;
- servidor de ficheiros - unidade de rede pessoal;
- servidor de ficheiros - unidade de rede departamental;
- servidor de ficheiros – unidade de rede da organização;
- aplicação de presença com acesso a *chat* e integração telefónica;

Dependendo do tipo de ligação/vinculo do utilizador com o município os privilégios de acesso são diferentes, de acordo com o descrito na tabela 8.

Perfil de utilizador	Privilégios
Funcionário	• Acesso à rede interna; • Acesso à rede sem fios; • Conta de correio eletrónico institucional; • Área de partilha de ficheiros comum; • Área de partilha de ficheiros de serviço; • Área pessoal para armazenamento de ficheiros; • Acesso ao portal intranet; • Acesso a aplicações de backoffice;
Estagiário	• Acesso à rede interna; • Acesso à rede sem fios; • Área de partilha de ficheiros comum; * Dependendo do tipo de estagiário pode ter acesso à área de partilha de ficheiros de serviço.
Convidados	• Acesso à rede sem fios; * Dependendo do tipo de convidado pode ter acesso à rede e interna e acesso a aplicações de backoffice;

Tabela 8: Privilégios de acesso por perfil de utilizador

4 Metodologia

4.1 Opções Metodológicas

O desenvolvimento de um trabalho de investigação pressupõe a utilização de técnicas e métodos científicos de forma de garantir o rigor do trabalho desenvolvido e do conhecimento gerado.

Num trabalho a definição do método de investigação está diretamente relacionada com o problema a ser estudado. Nesta situação específica recorreu-se ao estudo de caso por ser a opção metodológica que nos conduz ao alcance do objetivo preconizado para a dissertação: avaliação da segurança de Sistemas de Informação no Município de Torres Novas.

De acordo com Yin (2010), estudo de caso é "uma investigação empírica que investiga um fenômeno contemporâneo em profundidade e em seu contexto de vida real, especialmente quando os limites entre o fenômeno e o contexto não são claramente definidos" (Yin, 2010, p. 32).

Desta definição é importante destacar: "especialmente quando os limites entre o fenômeno e o contexto não são claramente definidos", uma vez que aqui está a justificação para a utilização do estudo de caso pois, quando numa investigação o local da aplicação é indiferente, pode-se optar por vários métodos, no entanto quando o fenómeno estudado não pode ser separado do contexto onde se dá trata-se de um estudo de caso.

Yin defende a escolha de estudo de caso como a estratégia preferida quando nos deparamos com questões que se focam no "como" e no "porquê" das coisas, quando o investigador tem pouco controlo sobre os eventos e quando o nosso objeto de análise se trata de um fenómeno atual analisado num contexto da vida real (Yin, 2010).

De acordo com Coutinho e Chaves (2002, p. 223), "A característica que melhor identifica e distingue esta abordagem metodológica é o facto de se tratar de um plano de investigação que envolve o estudo intensivo e detalhado de uma entidade bem definida: o "caso"."

Os mesmos autores referem ainda que, no estudo de caso, tal como a expressão indica, examina-se o "caso" (ou um pequeno número de "casos") em detalhe, em profundidade, no seu contexto natural, reconhecendo-se a sua complexidade e recorrendo-se para isso a todos os métodos que se revelem apropriados. A finalidade da investigação é sempre holística (sistémica, ampla, integrada) ou seja, visa preservar e compreender o "caso" no seu todo e na sua unicidade (Coutinho & Chaves, 2002).

Coutinho (2006), refere que quase tudo pode ser um "caso": um indivíduo, um personagem, um pequeno grupo, uma organização, uma comunidade ou mesmo uma nação.

Yin (2010) considera que o estudo de caso é utilizado em diversas situações, contribuindo para o conhecimento acerca de indivíduos, grupos e organizações, tanto a nível social, político como fenomenal, é igualmente útil para investigar novos conceitos, bem como para verificar como são aplicados e utilizados na prática elementos de uma teoria.

Coutinho (2006) considera que, a nível metodológico, a maioria dos autores classificam os estudos em qualitativos, quantitativos ou mistos.

Coutinho e Chaves (2002, p. 225) referem que devido ao facto de o estudo de caso

> ter um forte cunho descritivo, associado ao facto do investigador estar pessoalmente implicado no estudo, leva a que muitos tendam a associar o estudo de caso à investigação qualitativa o que é todavia uma conceção errada já que o estudo de caso pode também ser conduzido no quadro de outros paradigmas de investigação como o positivista ou mesmo o crítico (Ponte, 1994; Lessard Hébert, Goyette & Boutin, 1994; Punch, 1998), razão porque alguns autores a consideram como uma modalidade de investigação mista.

A investigação mista é a modalidade em que se insere o presente estudo, uma vez que a avaliação da segurança de Sistemas de Informação no Município de Torres Novas foi efetuada por especialistas tendo em conta a respetiva perceção da realidade, a sua interpretação do contexto, a sua forma de pensar e o seu ponto de vista (abordagem qualitativa), no entanto tiveram que atribuir uma classificação, fazer uma medição, baseada numa escala numérica que serviu de fundamentação para o calculo do nível de

maturidade médio por categoria de controlo, por secção de controlo e geral do Município (abordagem quantitativa).

Coutinho (2006, p. 5) define os estudos mistos como "todos os trabalhos de investigação que não se enquadram em nenhuma das duas categorias anteriores, seja por reuniram métodos de ambos, seja por possuírem individualidade própria derivada da inspiração num paradigma de investigação que não o positivista ou interpretativo".

Yin (2010) refere que os estudos de caso, podem incluir detalhes e até mesmo ser limitados a evidências quantitativas, não é o facto de a evidência ser quantitativa ou qualitativa que distingue o método de pesquisa.

Na verdade, uma das vantagens do estudo de caso assenta no facto de permitir a conjugação entre diferentes abordagens, nomeadamente das abordagens qualitativa e quantitativa permitindo utilizar variadas técnicas de recolha de informação, de forma a reunir informações numerosas, pormenorizadas com o objetivo de abarcar a totalidade da situação (Caixeiro, 2014).

No âmbito deste trabalho de investigação, pareceu-nos ser possível articular, combinar e conjugar as abordagens qualitativas e quantitativas, de forma a alcançar uma informação mais profunda e diversificada.

4.2 Técnicas e Instrumentos de Recolha de Dados

Na base das técnicas de recolha de dados estão ações fundamentais como observar, ler e perguntar.

No início deste estudo a observação direta foi uma das técnicas de recolha de dados idealizadas, a par com o inquérito. No entanto no desenvolver dos trabalhos surgiu a situação de pandemia de Covid-19 e as consequentes medidas decretadas pelo Governo Português para conter o surto, que implicaram uma adaptação de todos os setores da sociedade, inviabilizando a observação.

De facto, o encerramento de serviços, a rotatividade das equipas em trabalho presencial e o condicionamento da liberdade de circulação comprometeram profundamente a realização de trabalho de campo.

Deste modo, as técnicas de recolha de dados utilizadas neste estudo foram o inquérito por questionário (fonte principal) e a análise documental (fonte secundária, principalmente de apoio à compreensão do enquadramento da temática no Município).

Análise Documental:

Tendo em conta o objeto de estudo da presente investigação, a análise documental recaiu sobre a documentação que nos permitiu conhecer melhor o objeto de estudo, o meio envolvente.

Por outro lado, os documentos institucionais norteadores da vida organizacional, nomeadamente, os que referem procedimentos, que definem as principais responsabilidades e atividades desenvolvidas na área em questão, instruções, planos estratégicos, documentação técnica sobre a implementação, gestão operacional e manutenção dos Sistemas de Informação são uma importante ferramenta para compreender e interpretar os resultados obtidos no questionário.

A análise destes documentos permite-nos uma primeira aproximação à forma de funcionamento, perceber como são mobilizados os recursos, a cultura organizacional, as diretrizes emanadas pela liderança, quais as situações consideradas mais relevantes no quotidiano organizacional, o contexto de ação.

Inquérito por questionário

O inquérito por questionário é uma estratégia de pesquisa utilizada desde o final do século XVIII e início do século XIX, tornando-se a sua utilização ainda mais intensa após a segunda Guerra Mundial.

O questionário surge, frequentemente, associado à investigação quantitativa por medir determinados atributos de uma população e por o investigador recorrer a técnicas de análise estatística para o tratamento de dados.

A técnica de inquérito por questionário é mais do que a simples compilação de questões, a construção de um questionário exige do investigador esforço e atenção, as questões têm de refletir o objetivo que se quer verificar (Caixeiro, 2014).

O inquérito por questionário é uma técnica de recolha que se apoia numa série de questões estandardizadas e pré-determinadas que nos permite ter acesso a informação atual e atualizada, ou seja, esta técnica de pesquisa permite estudar um fenómeno tal como ele ocorre e é representado num determinado momento e deverá ser efetuado a pessoas que propiciem determinado conhecimento ao investigador.

As questões devem ter em consideração três princípios básicos: o Princípio da Clareza (devem ser claras, concisas e unívocas), Princípio da Coerência (devem corresponder à intenção da própria pergunta) e Princípio da Neutralidade (não devem induzir a uma resposta) (Barbosa, 2012).

O questionário pode ser composto por questões de resposta fechada ou de resposta aberta. As questões de resposta aberta permitem ao inquirido responder com as suas próprias palavras, havendo liberdade de expressão. Nas questões de resposta fechada o investigador determina previamente as diversas opções de resposta, limitando-se o inquirido a assinalar a (as) opção(ões) adequada(s). Também podem aparecerem questões dos dois tipos no mesmo questionário, sendo este considerado misto.

O preenchimento do questionário pode ser de administração direta, quando o preenchimento fica a cargo do próprio respondente, ou de administração indireta, quando o inquiridor regista a informação fornecida pelo respondente (Quivy & Campenhoudt, 1998). O método por administração direta permite que os inquiridos respondam no momento que lhes pareça mais apropriado e não os expõe à influência do investigador, (Almeida & Pinto, 1995).

Após a recolha dos dados o processo é completado por métodos de análise de dados, que vão permitir organizar, apresentar e descrever os dados abrindo caminho à interpretação de factos, à identificação de relações e padrões.

Neste estudo, em que o objetivo é medir a performance da Segurança da Informação no Município de Torres Novas, elaborou-se um questionário fundamentado na norma ISO/IEC 27002:2013, ao qual se associou um modelo de maturidade como escala, obtendo assim um questionário de resposta fechada, cujo preenchimento ficou a cargo do próprio respondente.

Fez-se corresponder a cada controlo (114 no total) uma questão cuja resposta apresenta numa escala de Likert entre 0 e 5, correspondendo à classificação do grau da maturidade. Foram fornecidas as diretrizes de implementação e a tabela com a discriminação dos seis níveis de maturidade para apoiar a resposta.

O inquérito foi submetido à apreciação e validação por dois especialistas da área.

Relativamente à estrutura do questionário das 14 cláusulas de controlos de segurança (A.5 a A.18), foram formuladas 114 questões, que corresponde ao número total de controlos presentes na ISO/IEC 27002:2013, com a distribuição apresentada na tabela 9:

Secção	Descrição	N.º de Objetivos de controlo	N.º de controlos (Questões)
A.5	Política de Segurança	1	2
A.6	Organização da Segurança da Informação	2	7
A.7	Segurança em Recursos Humanos	3	6
A.8	Gestão de Ativos	3	10
A.9	Controlo de Acesso	4	14
A.10	Criptografia	1	2
A.11	Segurança Física e do Ambiente	2	15
A.12	Segurança nas Operações	7	14
A.13	Segurança das Comunicações	2	7
A.14	Aquisição, Desenvolvimento e Manutenção de Sistemas	3	13
A.15	Relação com Fornecedores	2	5
A.16	Gestão de Incidentes de Segurança de Informação	1	7
A.17	Aspetos da Segurança da Informação na Gestão da Continuidade do Negócio	2	4
A.18	Conformidade	2	8
TOTAL		**35**	**114**

Tabela 9: Relação do número de questões formuladas por secção

A estrutura do questionário (figura 15) foi baseada na estrutura da norma (figura 14).

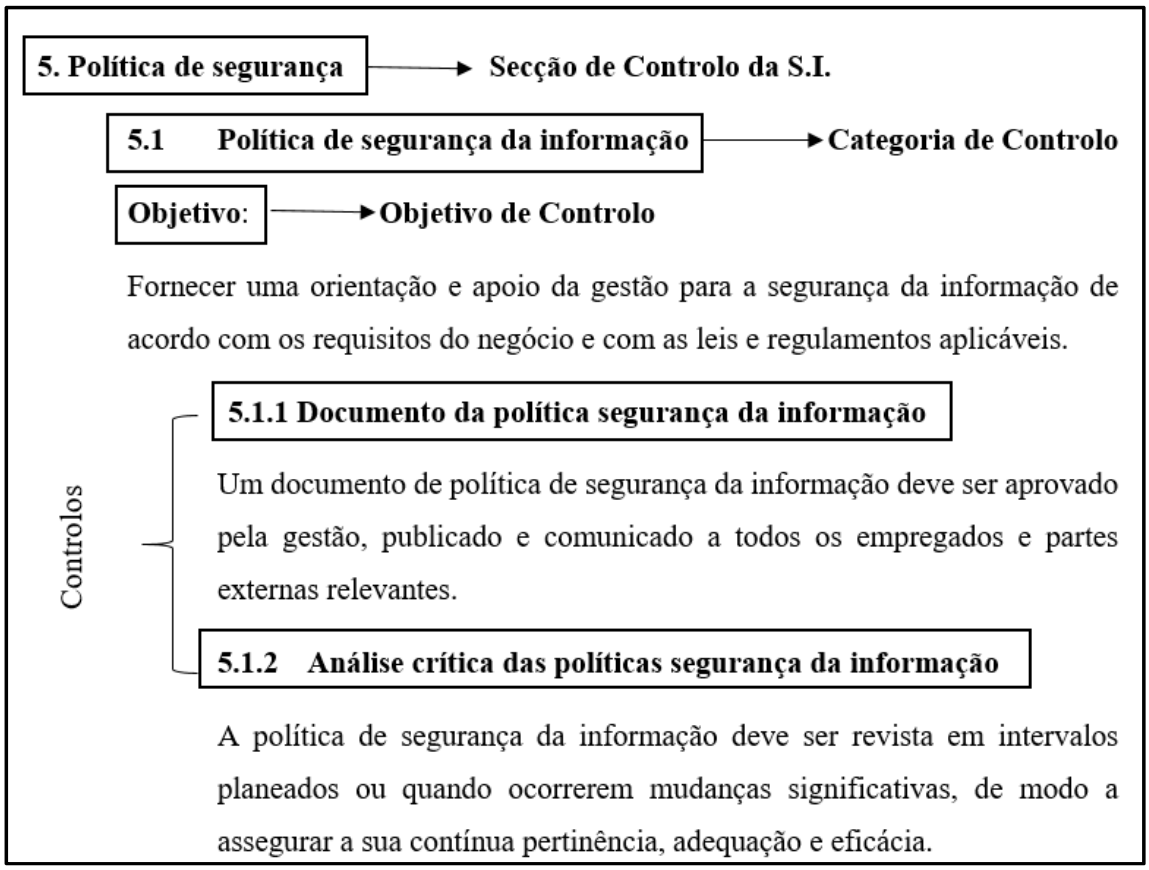

Figura 13: Estrutura da norma

A.5 Política de segurança

A.5.1 Política de segurança da informação

Objetivo: Proporcionar uma orientação e apoio da gestão para a segurança da informação de acordo com os requisitos de negócio e com as leis e regulamentações aplicáveis.

Standard		Controlo	Nível CMMI
A.5.1.1	Documento da política de segurança da informação	Um documento de política de segurança da informação deve ser aprovado pela gestão, publicado e comunicado a todos os empregados e partes externas relevantes.	0 1 2 3 4 5
		Notas:	
A.5.1.2	Análise crítica das políticas de segurança da informação	A política de segurança da informação deve ser revista em intervalos planeados ou quando ocorrerem mudanças significativas, de modo a assegurar a sua contínua pertinência, adequação e eficácia.	0 1 2 3 4 5
		Notas:	

Figura 14: Estrutura do questionário

Constituem-se como inquiridos deste estudo dois especialistas de informática:

Especialista A: Formação académica em engenharia informática e especialização em redes e sistemas de comunicação, com 48 anos e 17 anos de experiência na área.

Especialista B: Formação académica em Tecnologias da Informação e Comunicação, com 41 anos e 21 anos de experiência na área.

O questionário foi aplicado entre junho e outubro de 2020.

4.3 Procedimentos de Análise e Tratamento de Dados

Após a recolha de dados, segue-se a organização, tratamento e apresentação dos mesmos, ou seja, a estruturação de um conjunto de informações a partir das quais se podem extrair conclusões e tomar decisões.

Isto porque, os dados obtidos nos questionários, por si mesmos, são insuficientes para extrair conclusões, têm se ser analisados, isto é, organizados e estruturados de forma a transformarem-se em informação esclarecedora.

Segundo Erickson (1986) é na fase em que se analisam os materiais recolhidos que se pode falar de dados de investigação, uma vez que o conjunto do material compilado no campo não é, em si mesmo, um conjunto de dados, mas sim, uma fonte de dados.

A análise dos questionários e tratamento de dados foi efetuada recorrendo-se ao auxílio de Folha de Cálculo (Microsoft Excel), onde foi efetuada a estatística descritiva. Com base nas respostas chegou-se a um nível de maturidade médio por categoria de controlo, por secção de controlo e geral. A partir dos resultados obtidos é possível perceber em que ponto se encontra o Município em termos de Segurança dos Sistemas de Informação, efetuar uma análise detalhada e verificar quais as lacunas, as vulnerabilidades, as áreas mais fracas e as mais fortes, bem como identificar os pontos de melhoria.

5 Análise dos Resultados

5.1 Resultados do Inquérito

Os resultados da análise efetuada ao inquérito estão evidenciados na tabela 10, onde é apresentada a maturidade média por controlo e a maturidade média geral do MTN.

Controlo	Descrição	Maturidade Média	Maturidade Média Geral
A.5	Política de Segurança	3,00	
A.6	Organização da Segurança da Informação	3,15	
A.7	Segurança em Recursos Humanos	3,00	
A.8	Gestão de Ativos	2,83	
A.9	Controlo de Acesso	3,90	
A.10	Criptografia	3,50	
A.11	Segurança Física e do Ambiente	3,19	
A.12	Segurança nas Operações	4,00	**3,21**
A.13	Segurança das Comunicações	3,67	
A.14	Aquisição, Desenvolvimento e Manutenção de Sistemas	3,11	
A.15	Relação com Fornecedores	2,58	
A.16	Gestão de Incidentes de Segurança de Informação	2,14	
A.17	Aspetos da Segurança. da informação na Gestão da Continuidade do Negócio	3,50	
A.18	Conformidade	3,37	

Tabela 10: Avaliação geral e por secção, efetuada com base no modelo de maturidade

O gráfico 1 apresenta os níveis médios de maturidade apurados para cada uma das catorze secções, de onde se destacam a secções A.9 – controlo de acessos e a secção A.12 – segurança das operações com os níveis mais elevados de maturidade e a secção A.16 – gestão de incidentes de Segurança da Informação com o nível de maturidades mais baixo.

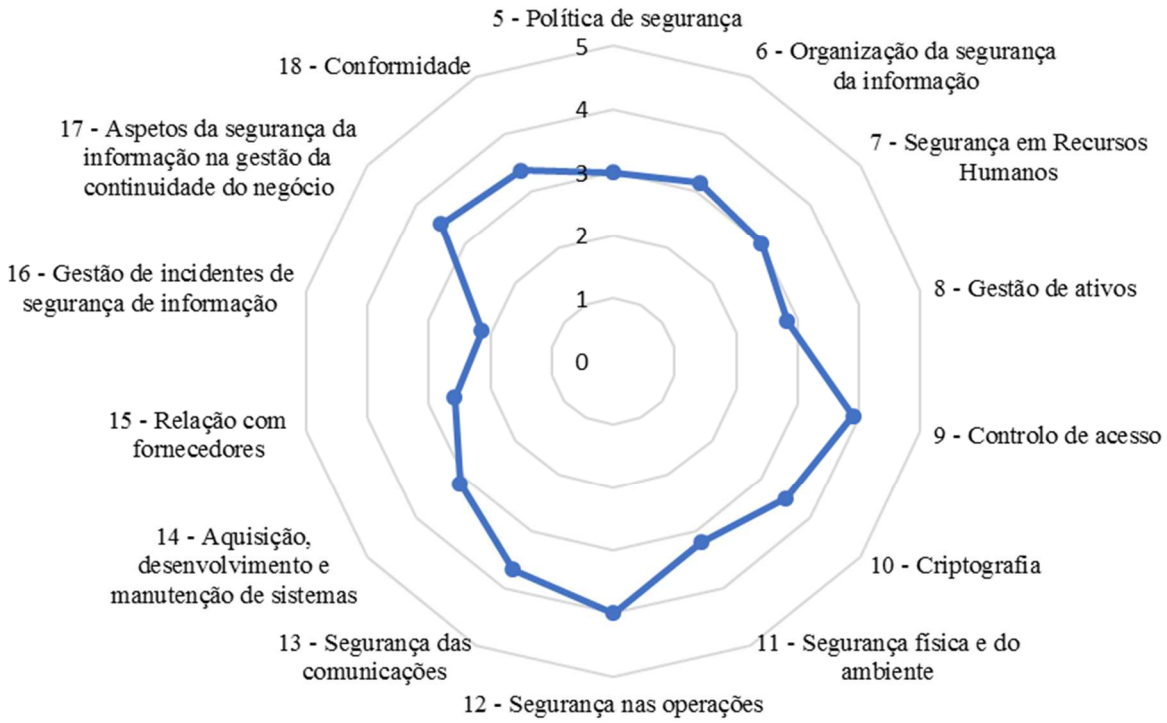

Gráfico 1: Representação gráfica do nível médio de maturidade apurado por secção

Através da análise dos resultados obtidos no inquérito, considera-se que o Município de Torres Novas possui um nível de maturidade médio geral de 3, mais concretamente 3,21, o que significa que, em média, os seus procedimentos de segurança estão definidos, mas existem procedimentos a melhorar para aprofundar a segurança dos Sistemas de Informação. Os processos estão normalizados e documentados e são divulgados em formação. É obrigatório que os processos sejam seguidos, pelo que é improvável que sejam detetados desvios. Os processos não são sofisticados, mas existe a formalização das práticas existentes.

5.2 Análise dos Resultados Obtidos

Por uma questão de segurança e confidencialidade, na análise detalhada dos resultados obtidos no inquérito, serão omitidas as classificações atribuídas por controlo, apresenta-se apenas a classificação média por secção e por objetivo de controlo.

Para cada secção será feita uma análise dos pontos que se destacam e que mais contribuem para a caracterização do estado atual da Segurança da Informação do MTN, sempre que se detetem fragilidades recomendar-se-ão ações corretivas.

Controlo	Descrição	Maturidade Média
A.5	**Política de segurança**	**3,00**
A.5.1	**Política de segurança da informação**	**3,00**
A.5.1.1	Documento da política segurança da informação	
A.5.1.2	Análise crítica das políticas segurança da informação	

Tabela 11: Avaliação da maturidade média da secção A.5 e discriminação dos controlos avaliados

Como se verifica na tabela 11 o MTN apresenta um grau médio de maturidade 3 relativamente à política de segurança.

Verifica-se que o MTN possui um documento onde estão definidas as políticas de segurança (Regulamento Interno da Informática), este documento foi aprovado em reunião de câmara e é do conhecimento de todos os colaboradores. No entanto, o mesmo não é revisto com regularidade, apesar de as políticas de segurança serem ajustadas sempre que necessário o documento não acompanha estas atualizações.

Recomenda-se que o regulamento seja revisto e atualizado, de forma a espelhar a realidade das políticas de segurança adotadas, só assim se assegura a sua contínua pertinência, adequação e eficácia.

Controlo	Descrição	Maturidade Média
A.6	**Organização da segurança da informação**	**3,15**
A.6.1	**Organização interna**	**2,80**
A.6.1.1	Responsabilidades e papéis pela segurança da informação	
A.6.1.2	Segregação de funções	
A.6.1.3	Contacto com autoridades	
A.6.1.4	Contacto com grupos especiais	
A.6.1.5	Segurança da informação na gestão de projetos	
A.6.2	**Dispositivos móveis e trabalho remoto**	**3,50**
A.6.2.1	Política para o uso de dispositivo móvel	
A.6.2.2	Trabalho remoto	

Tabela 12: Avaliação da maturidade média da secção A.6 e descriminação dos controlos avaliados

A secção A.6, apresentada na tabela 12, preocupa-se com a gestão da Segurança da Informação dentro da organização e contém 6 controlos que fornecem orientações nesse sentido.

Relativamente às orientações desta secção verifica-se que no MTN as responsabilidades pela Segurança da Informação estão atribuídas e bem definidas, mas não formalmente.

Seguindo as recomendações do controlo A.6.1.1 o MTN deverá definir claramente as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de Segurança da Informação específicos, deverá ainda associar orientações detalhadas às responsabilidades.

O mesmo controlo recomenda ainda que as pessoas com responsabilidades definidas pela Segurança da Informação devem delegar as tarefas de Segurança da Informação para outros, continuando responsáveis por verificar se as tarefas delegadas estão a ser executadas corretamente. Esta delegação de tarefas não se verifica no MTN.

A segregação de funções é uma preocupação no MTN e encontra-se bem implementada.

Verifica-se que o MTN não possui um procedimento que especifique quando e quais as autoridades a ser contactadas em caso de incidente de Segurança da Informação, situação que deverá ser corrigida.

O MTN mantém um reduzido contacto com associações, grupos especializados ou fóruns da área de Segurança da Informação, situação que deverá ser colmatada pois estes contactos são muito úteis para ampliar conhecimentos sobre as melhores práticas, para os especialistas do MTN se manterem atualizados, receberem previamente alertas, ter acesso a consultoria especializada em Segurança da Informação.

A Segurança da Informação na gestão de projetos é sempre considerada pela DTICMA, no entanto, os promotores dos projetos nem sempre têm esta preocupação, situação que deverá ser melhorada através de sensibilização e formação interna.

No que se refere ao trabalho remoto falta identificar e documentar por escrito as regras e políticas para que sejam incluídas no Regulamento Interno da Informática, esta questão revelou-se de grande importância na situação pandémica que se está a viver.

Controlo	Descrição	Maturidade Média
A.7	**Segurança em Recursos Humanos**	**3,00**
A.7.1	**Antes da contratação**	**4,00**
A.7.1.1	Seleção	
A.7.1.2	Termos e condições de contratação	
A.7.2	**Durante a contratação**	**2,00**
A.7.2.1	Responsabilidades da gestão	
A.7.2.2	Consciencialização, educação e formação em segurança da informação	
A.7.2.3	Processo disciplinar	
A.7.3	**Rescisão ou mudança de contrato**	**3,00**
A.7.3.1	Responsabilidades pela rescisão ou mudança de contrato	

Tabela 13: Avaliação da maturidade média da secção A.7 e discriminação dos controlos avaliados

Na tabela 13 são apresentados os valores médios de maturidade apurados para a secção A.7 que tem como preocupação a segurança em recursos humanos.

A seleção e as condições de contratação são procedimentos devidamente instituídos na instituição e obedecem a regras bem definidas decorrentes de obrigações legais.

Recomenda-se uma maior consciencialização para a problemática da Segurança da Informação através de ações de formação interna para todos os recursos humanos do MTN.

Ao nível do processo disciplinar verifica-se que não está documentado nem prevista a existência de um processo formal, situação que deverá ser revista, uma vez que as boas práticas recomendam a existência de um processo disciplinar implementado e comunicado a aplicar a funcionários que cometam uma violação de Segurança da Informação.

Relativamente à rescisão ou mudança de contrato verifica-se que nem sempre a DTICMA é informada no momento em que estas ocorrerem, o que pode implicar, durante algum período, falhas no controlo da segurança neste ponto. Deverá ser definido um circuito interno e identificados os responsáveis por informar a DTICMA quando ocorrem rescisões ou mudanças de contrato, este procedimento deverá ser incluído no Regulamento Interno da Informática.

Controlo	Descrição	Maturidade Média
A.8	**Gestão de ativos**	**2,83**
A.8.1	**Responsabilidade pelos ativos**	**4,50**
A.8.1.1	Inventário dos ativos	
A.8.1.2	Proprietário dos ativos	
A.8.1.3	Uso aceitável dos ativos	
A.8.1.4	Devolução dos ativos	
A.8.2	**Classificação da informação**	**3,00**
A.8.2.1	Classificação da informação	
A.8.2.2	Rotulagem e tratamento da informação	
A.8.2.3	Tratamento dos ativos	
A.8.3	**Tratamento de dispositivos de armazenamento de informaçã**	**1,00**
A.8.3.1	Gerir os meios de comunicação removíveis	
A.8.3.2	Rotulagem e tratamento da informação	
A.8.3.3	Transferência física dos meios de comunicação	

Tabela 14: Avaliação da maturidade média da secção A.8 e discriminação dos controlos avaliados

A preocupação central da secção A.8 é manter os ativos da organização adequadamente protegidos. Como é possível verificar na tabela 14 o MTN apresenta um nível da maturidade médio de 2,83, sendo uma das secções que está abaixo da média.

Relativamente aos ativos associados à informação, os chamados ativos primários (processos e atividades de negócio, informação) é utilizado um sistema de gestão documental onde estão contidos todos os documentos gerados na execução dos processos, permitindo a associação de qualquer ficheiro em formato eletrónico. Este sistema de gestão permite constituir um arquivo digital corrente, intermédio e histórico de acordo com as normas legais estabelecidas.

Associada a cada documento integrado no sistema de gestão documental acima referido existe uma classificação da informação, no entanto esta está a ser revista e melhorada, o que implica que, provavelmente, nem toda a informação tem a classificação mais adequada.

Por sua vez, os ativos associados aos recursos de processamento da informação, os designados ativos secundários, (*hardware*, *software*, rede, etc…) encontram-se todos

inventariados, com um responsável associado e com regras de utilização e devolução definidas no Regulamento Interno da Informática.

O objetivo A.8.3 tem a classificação de 1, situação que se deve ao facto de não existir um procedimento documentado relativo à utilização de dispositivos amovíveis de armazenamento de dados, situação que deverá ser corrigida

Deverão ser documentados e implementados procedimentos que definam as regras desde a utilização até à eliminação de dispositivos amovíveis de armazenamento de dados de forma a prevenir a divulgação não autorizada, a modificação, remoção ou destruição de informação armazenada nestes dispositivos.

Controlo	Descrição	Maturidade Média
A.9	**Controlo de acesso**	**3,90**
A.9.1	**Requisitos do negócio para controlo de acesso**	**4,00**
A.9.1.1	Política de controlo de acessos	
A.9.1.2	Acesso às redes e aos serviços de redes	
A.9.2	**Gestão de acesso dos utilizadores**	**4,00**
A.9.2.1	Registo e cancelamento de utilizadores	
A.9.2.2	Fornecimento de acesso ao utilizador	
A.9.2.3	Gestão de direitos de acesso privilegiados	
A.9.2.4	Gestão da informação secreta de autenticação dos utilizadores	
A.9.2.5	Revisão dos direitos de acesso dos utilizadores	
A.9.2.6	Remoção ou ajustamento dos direitos de acesso	
A.9.3	**Responsabilidade dos utilizadores**	**3,00**
A.9.3.1	Utilização da informação secreta de autenticação	
A.9.4	**Controlo de acesso aos sistemas e às aplicações**	**4,60**
A.9.4.1	Restrição de acesso à informação	
A.9.4.2	Procedimentos seguros de entrada no sistema (log-on)	
A.9.4.3	Sistema de gestão de senha	
A.9.4.4	Uso de programas utilitários privilegiados	
A.9.4.5	Controlo de acesso ao código-fonte de programas	

Tabela 15: Avaliação da maturidade média da secção A.8 e discriminação dos controlos avaliados.

A secção A.9 - controlo de acesso, é a segunda secção mais bem classificada, com um nível médio de maturidade de 3,90, como é possível verificar na tabela 15.

Os recursos humanos do MTN apenas têm acesso à informação e aos recursos de processamento da informação que a DTICMA autoriza. O fornecimento dos acessos necessários é solicitado, por escrito, pelos superiores hierárquicos à DTICMA e as configurações dos acessos são efetuadas pelos técnicos responsáveis em cada sistema informático.

Tal como já referido na análise à secção A.7 – segurança de recursos humanos, verifica-se que, por vezes, quando ocorrem situações de cessação de emprego, contrato ou acordo, a DTICMA não é informada no imediato, podendo assim eventualmente implicar, durante algum período de tempo, falhas no controlo de segurança.

Recomenda-se que seja definido um circuito interno e identificados os responsáveis por informar a DTICMA quando ocorrem situações de cessação de emprego, contrato ou acordo. Este procedimento deverá ser incluído no Regulamento Interno da Informática.

Relativamente à responsabilidade dos utilizadores verificam-se algumas situações de *post-it* com *passwords* colados no ecrã.

Recomenda-se uma maior consciencialização para a importância da proteção das informações de autenticação através de ações de formação interna para todos os recursos humanos do MTN.

O acesso aos sistemas e às aplicações é feito através de *login/password* que obrigam a políticas de *password* segura impedindo o uso de *passwords* simples e exigindo a sua alteração frequente.

Controlo	Descrição	Maturidade Média
A.10	**Criptografia**	**3,50**
A.10.1	**Controlos criptográficos**	**3,50**
A.10.1.1	Política para o uso de controlos criptográficos	
A.10.1.2	Gestão de chaves criptográficas	

Tabela 16: Avaliação da maturidade média da secção A.10 e discriminação dos controlos avaliados

A secção A.10, apresentada na tabela 16 é composta por dois controlos cuja preocupação é a criptografia e o seu nível médio de maturidade é 3,50.

O MTN utiliza controlos criptográficos para a proteção da informação, estando atualmente em curso a migração de sistemas sobretudo de acesso externo para sistemas com criptografia.

Os certificados das chaves criptográficas são alterados em períodos inferiores a 3 meses.

Controlo	Descrição	Maturidade Média
A.11	**Segurança física e do ambiente**	**3,19**
A.11.1	**Áreas de segurança**	**3,50**
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 do meio-ambiente	
A.11.1.5	Trabalho em áreas seguras	
A.11.1.6	Áreas de entrega e de carregamento	
A.11.2	**Equipamentos**	**2,89**
A.11.2.1	Escolha de local e proteção do equipamento	
A.11.2.2	Serviços de apoio	
A.11.2.3	Segurança da cablagem de rede	
A.11.2.4	Manutenção dos equipamentos	
A.11.2.5	Remoção de ativos	
A.11.2.6	Segurança de equipamentos e ativos fora das dependências da organização	
A.11.2.7	Reutilização e alienação segura de equipamentos	
A.11.2.8	Equipamentos de utilizadores sem monitorização	
A.11.2.9	Política de mesa limpa e tela limpa	

Tabela 17: avaliação da maturidade média da secção A.11 e discriminação dos controlos avaliados

A secção A.11, apresentada na tabela 17, tem como preocupação centrar a segurança física e do ambiente.

O MTN possui edifícios distribuídos pela cidade, verificando-se que, em alguns deles, não existe um adequado controlo de acesso e circulação de pessoas externas.

As salas com equipamento informático crítico, centro de dados e salas técnicas têm meios de controlo de acesso restritos, possuem alarme e o acesso é permitido apenas aos técnicos responsáveis pela administração de sistemas.

Sugere-se que sejam aplicadas, a todos os edifícios do MTN, medidas que assegurem que apenas pessoas autorizadas entram e circulam nas instalações.

Nem todos os equipamentos estão protegidos contra falhas de energia elétrica e alguns edifícios, mais antigos, não estão preparados para ter cablagem de rede (que transporta dados ou dá suporte aos serviços de informação) que permita uma proteção adequada contra intercetação, interferência ou danos.

As medidas de segurança para ativos que operem fora das dependências do MTN requer melhorias

Relativamente à política mesa limpa e ecrã limpo esta ainda não foi interiorizada pelos recursos humanos do MTN, pelo que se recomenda uma maior consciencialização para a importância desta temática através da realização de ações de formação interna promovidas pela DTICMA.

Controlo	Descrição	Maturidade Média
A.12	**Segurança nas operações**	**4,00**
A.12.1	**Responsabilidades e procedimentos operacionais**	**3,75**
A.12.1.1	Documentação dos procedimentos de operação	
A.12.1.2	Gestão de mudanças	
A.12.1.3	Gestão de capacidade	
A.12.1.4	Separação dos ambientes de desenvolvimento, teste e operacionais	
A.12.2	**Proteção contra vírus**	**4,00**
A.12.2.1	Controlos contra malware	
A.12.3	**Cópias de segurança**	**4,00**
A.12.3.1	Cópias de segurança das informações	
A.12.4	**Registo de eventos (Log) e monitorização**	**3,25**
A.12.4.1	Registo de eventos	
A.12.4.2	Proteção da informação logs	
A.12.4.3	Registo de eventos (log) de administrador e operador	
A.12.4.4	Sincronização dos relógios	
A.12.5	**Controlo de software operacional**	**5,00**
A.12.5.1	Instalação de software nos sistemas operacionais	
A.12.6	**Gestão de vulnerabilidades técnicas**	**4,00**
A.12.6.1	Gestão de vulnerabilidades técnicas	
A.12.6.2	Restrições quanto à instalação de software	
A.12.7	**Considerações quanto à auditoria de Sistemas de informação**	**4,00**
A.12.7.1	Controlos de auditoria de sistemas de informação	

Tabela 18: avaliação da maturidade média da secção A.12 e discriminação dos controlos avaliados

A secção A.12, apresentada na tabela 18, tem como objetivo principal garantir um funcionamento seguro e correto dos recursos de processamento da informação. No MTN esta é uma área em que, em média, os procedimentos de segurança são monitorizados, é mensurada a conformidade com os procedimentos instituídos e são efetuadas melhorias frequentes.

A DTICMA tem adotado como forma de atuação, sempre que surgem novos procedimentos ou a necessidade de alteração de procedimentos já existentes, a

publicação, na intranet e em local de destaque, de manuais de utilização, garantindo assim que todos os utilizadores têm conhecimento imediato dos novos procedimentos.

O *backup* (sistema de cópias de segurança) é feito ao longo do dia do servidor instalado no centro de dados do MTN para um servidor que está noutra localização. Ao fim de semana, este servidor cria uma réplica, das cópias de segurança alojadas, para banda magnética. No início da semana seguinte esta réplica é armazenada numa terceira localização segura. Desta forma, seguindo as melhores práticas de *Disaster Recovery*, caso ocorram situações de catástrofe ou desastre que tornem o centro de dados indisponível é possível garantir a recuperação dos dados.

Os registos (*log*) das atividades dos utilizadores não são analisados criticamente e revistos regularmente. Geralmente esta situação só ocorre quando é detetado algum problema. O mesmo acontece com os registos de eventos (*log*) de administradores e operadores do sistema.

Controlo	Descrição	Maturidade Média
A.13	**Segurança das comunicações**	**3,67**
A.13.1	**Gestão da segurança em redes**	**4,33**
A.13.1.1	Controlos de redes	
A.13.1.2	Segurança dos serviços de redes	
A.13.1.3	Segregação de redes	
A.13.2	**Transferência de informação**	**3,00**
A.13.2.1	Politicas e procedimentos para transferência de informações	
A.13.2.2	Acordos para transferência de informações	
A.13.2.3	Mensagens eletrónicas	
A.13.2.4	Acordos de confidencialidade e não divulgação	

Tabela 19: Avaliação da maturidade média da secção A.13 e discriminação dos controlos avaliados

A tabela 19 apresenta os resultados apurados para a secção A.13, que tem como preocupação central garantir a proteção das informações em redes e dos recursos de processamento da informação que os apoiam.

No MTN existem procedimentos e controlos estabelecidos para manter a Segurança da Informação transferida dentro da organização e com entidades externas.

No entanto, recomenda-se que os acordos de confidencialidade e não divulgação sejam analisados criticamente de forma a que reflitam as necessidades de proteção das informações confidenciais nas relações do MTN com as partes externas e funcionários.

Os acordos de confidencialidade e não divulgação têm como objetivo proteger as informações do MTN e informam os signatários das suas responsabilidades, para proteger, usar e divulgar a informação de forma responsável e autorizada. Pode ser necessária a utilização de diferentes formas de acordos de confidencialidade ou de não divulgação, devendo ser considerados os seguintes elementos:

a) definição da informação a ser protegida (por exemplo, informação confidencial);
b) o tempo de duração esperado de um acordo, incluindo situações onde a confidencialidade tenha que ser mantida indefinidamente;
c) ações requeridas quando um acordo está encerrado;
d) responsabilidades e ações dos signatários para evitar a divulgação não autorizada da informação;
e) o proprietário da informação, segredos comerciais e de propriedade intelectual, e como isto se relaciona com a proteção da informação confidencial;
f) o uso permitido da informação confidencial, e os direitos do signatário para usar a informação;
g) o direito de auditar e monitorizar as atividades que envolvam as informações confidencias;
h) o processo para notificação e relato de divulgação não autorizada das informações confidenciais;
i) termos para a informação ser devolvida ou destruída quando do término do acordo;
j) ações esperadas a serem tomadas no caso de uma violação deste acordo.

Controlo	Descrição	Maturidade Média
A.14	**Aquisição, desenvolvimento e manutenção de sistemas**	**3,11**
A.14.1	**Requisitos de segurança de sistemas de informação**	**3,67**
A.14.1.1	Análise e especificação dos requisitos de segurança da informação	
A.14.1.2	Serviços de aplicação seguros em redes públicas	
A.14.1.3	Proteger as transações em serviços de aplicações	
A.14.2	**Segurança em processos de desenvolvimento e de suporte**	**2,67**
A.14.2.1	Politica de desenvolvimento seguro	
A.14.2.2	Procedimentos para controlo de mudanças de sistemas	
A.14.2.3	Análise crítica técnica das aplicações após mudanças nas plataformas operacionais	
A.14.2.4	Restrições sobre mudanças em pacotes de software	
A.14.2.5	Princípios para projetar sistemas seguros	
A.14.2.6	Ambiente seguro para desenvolvimento	
A.14.2.7	Desenvolvimento subcontratado (Outsourcing)	
A.14.2.8	Teste de segurança do sistema	
A.14.2.9	Teste de aceitação de sistemas	
A.14.3	**Dados para testes**	**3,00**
A.14.3.1	Proteção de dados para teste	

Tabela 20: Avaliação da maturidade média da secção A.14 e discriminação dos controlos avaliados

Com esta secção pretende-se garantir que a Segurança da Informação é parte integrante de todo o ciclo de vida dos Sistemas de Informação, sendo para isso necessário assegurar que os projetos de informação e atividades de suporte são conduzidos, desde o seu inicio, tendo em conta a Segurança da Informação e respeitando as políticas da organização.

Como é pode ser observado na tabela 20, como pontos frágeis nesta secção destacam-se os controlos A.14.2.7, 14.2.8 e A.14.2.9, verificando-se que os testes de segurança e de aceitação efetuados, de uma forma geral, resumem-se ao mínimo necessário para que se possa avançar com a sua utilização.

Relativamente ao desenvolvimento de sistemas por entidades externas (*outsourcing*) (A.14.2.7) devem ser tidos em conta os seguintes pontos:

a) acordos de licença, propriedade do código e direitos de propriedade intelectual relacionado com o conteúdo fornecido (A.18.1.2);
b) requisitos contratuais para um projeto seguro, práticas de código e teste (A.14.2.1);

c) fornecimento de um modelo de ameaça aprovado para o desenvolvimento externo;
d) teste de aceitação relativos à qualidade e exatidão dos itens entregues;
e) fornecimento de evidência de que os princípios de segurança foram usados, para estabelecer um nível mínimo de segurança aceitável e a qualidade da privacidade;
f) fornecimento de evidências de que testes suficientes foram realizados para proteger contra a ausência de conteúdo malicioso, tanto intencional como não intencional no momento da entrega;
g) fornecimento de evidências de que testes suficientes foram aplicados para proteger contra presença de vulnerabilidades conhecidas;
h) acordos de garantia, por exemplo se o código fonte não está mais disponível;
i) direitos contratuais para auditar os controlos e processos de desenvolvimento;
j) documentação efetiva da construção do ambiente usado para realizar as entregas;
k) a organização permanece responsável pela conformidade com as leis aplicáveis e a verificação da eficácia dos controlos.

No que respeita aos testes de segurança do sistema (A14.2.8) convém que sejam realizados testes de funcionalidades de segurança durante o desenvolvimento de sistemas.

Novos sistemas ou atualizações requerem verificação e testes completos durante o processo de desenvolvimento, incluindo a preparação de um programa de atividade detalhado, com testes de entrada e de saída esperados sob determinadas condições. A abrangência do teste deve ser proporcional à importância e natureza do sistema.

Relativamente aos testes de aceitação de sistemas (A.14.2.9) devem ser efetuados para novos sistemas e novas versões. Devem incluir testes de requisitos de Segurança da Informação (A.14.1.1 e A.14.1.2) e adesão às práticas de desenvolvimento seguro de sistemas (A.14.2.1).

Os testes devem ser realizados em ambiente de teste realístico, de forma a assegurar que os testes são confiáveis e que o sistema não irá introduzir vulnerabilidades no ambiente do MTN.

Controlo	Descrição	Maturidade Média
A.15	**Relação com fornecedores**	**2,58**
A.15.1	**Segurança da informação na cadeia de fornecedores**	**2,67**
A.15.1.1	Política de segurança da informação no relacionamento com os fornecedores	
A.15.1.2	Abordar a segurança dentro dos contratos com fornecedores	
A.15.1.3	Fornecimento de tecnologias de informação e comunicação	
A.15.2	**Gestão da entrega do serviço do fornecedor**	**2,50**
A.15.2.1	Monitorização e revisão dos serviços de fornecedores	
A.15.2.2	Gestão de alterações nos serviços de fornecedores	

Tabela 21: Avaliação da maturidade média da secção A.15 e discriminação dos controlos avaliados

A secção 15, da qual os resultados de avaliação são apresentados na tabela 21, tem como preocupação garantir a proteção dos ativos da organização que estão acessíveis aos fornecedores.

Destes controlos, o A.15.1.3 e o A.15.2.1 são os que apresentam maturidade mais baixa, merecendo assim especial atenção.

Relativamente ao controlo A.15.1.3 não existe um procedimento normalizado para aplicar ao fornecimento de produtos e serviços de Tecnologia de Informação e Comunicação. Existe uma preocupação a este nível, mas não havendo um procedimento documentado, que tenha que ser obrigatoriamente seguido, é provável que ocorram falhas.

Sugere-se que, na revisão dos acordos com os fornecedores, sejam tidos em consideração os seguintes tópicos:

a) definição dos requisitos de Segurança da Informação aplicáveis na aquisição de serviços ou produtos de Tecnologia de Informação e Comunicação, em acréscimo aos requisitos de Segurança da Informação gerais, na relação com os fornecedores;

b) para os serviços de Tecnologia de Informação e Comunicação, exigir que o fornecedor divulgue os requisitos de Segurança da Informação da organização em toda a cadeia de fornecimento, caso os subfornecedores façam parte do serviço de Tecnologia de Informação e Comunicação a ser fornecido para a organização;

c) para produtos de Tecnologia de Informação e Comunicação, exigir que os fornecedores divulguem as práticas de Segurança da Informação apropriadas ao longo de toda a cadeia de fornecimento, caso esses produtos incluam componentes comprados a outros fornecedores;

d) implementação de um processo de monitorização e métodos aceitáveis para validação se os serviços e produtos de Tecnologia de Informação e Comunicação entregues estão aderentes aos requisitos de Segurança da Informação estabelecidos;

e) implementação de um processo para identificação dos componentes do serviço ou produto que são críticos para manter a funcionalidade e, portanto, requerem uma maior atenção e verificação quando construídos fora da organização, especialmente se o fornecedor principal adquirir partes dos componentes do serviço ou produto a outros fornecedores;

f) obtenção de garantia de que os componentes críticos e as suas origens podem ser rastreadas ao longo de toda a cadeia de fornecimento;

g) obtenção de garantia de que os produtos de Tecnologia de Informação e Comunicação entregues funcionam de acordo com o esperado, sem quaisquer características não desejadas ou não esperadas;

h) definição de regras para a partilha da informação relativamente a cadeia de fornecimento e quaisquer questões potenciais e compromissos assumidos entre a organização e os fornecedores;

i) a implementação de processos específicos para a gestão dos riscos de segurança associados, à disponibilidade e ao ciclo de vida dos componentes de Tecnologia de Informação e Comunicação. Isto inclui a gestão dos riscos de componentes quando estes deixarem de estar disponíveis, devido à saída do fornecedor do mercado ou por o fornecedor deixar de fornecer esses componentes devido aos avanços da tecnologia.

Relativamente à monitorização e análise critica dos serviços fornecidos, controlo A.15.2.1, apesar de existir uma preocupação com este controlo não existe um procedimento documentado e implementado, nem é efetuado em intervalos regulares.

A monitorização e análise crítica dos serviços fornecidos deve garantir que os termos e condições incluídos nos acordos de Segurança da Informação são cumpridos e que os incidentes e problemas de segurança são geridos de forma apropriada.

O relacionamento entre o MTN e os fornecedores devem obedecer a um processo de gestão que permita:

a) monitorizar os níveis de desempenho de serviço para verificar conformidade aos acordos;

b) analisar criticamente os relatórios de serviços produzidos por fornecedores e agendamento de reuniões de progresso conforme requerido pelos acordos;

c) realizar auditorias aos fornecedores, em conjunto com a análise crítica dos relatórios de auditoria independente, quando disponíveis, bem como o acompanhamento das questões identificadas;

d) fornecer informações sobre incidentes de segurança de informação e analisar criticamente tais informações, conforme requerido pelos acordos e por quaisquer procedimentos e diretrizes que os apoiem;

e) analisar criticamente os circuitos de auditoria do fornecedor e registos de eventos de Segurança da Informação, problemas operacionais, falhas, investigação de falhas e interrupções relativas ao serviço entregue;

f) resolver e gerir quaisquer problemas identificados;

g) analisar criticamente os aspetos de Segurança da Informação na relação dos fornecedores com seus próprios fornecedores;

h) garantir que o fornecedor mantém capacidade de serviço suficiente em conjunto com planos de trabalho desenhados para assegurar que os níveis de continuidade do serviço acordados são mantidos, no caso de um desastre ou falha dos serviços principais (A.17).

Controlo	Descrição	Maturidade Média
A.16	**Gestão de incidentes de segurança de informação**	**2,14**
A.16.1	**Gestão de incidentes de segurança da informação e melhorias**	**2,14**
A.16.1.1	Responsabilidades e procedimentos	
A.16.1.2	Notificação de eventos de segurança da informação	
A.16.1.3	Reportar fragilidades de segurança da informação	
A.16.1.4	Avaliação e decisão sobre eventos de segurança da informação	
A.16.1.5	Resposta aos incidentes de segurança da informação	
A.16.1.6	Aprender com os incidentes de segurança de informação	
A.16.1.7	Recolha de provas	

Tabela 22: Avaliação da maturidade média da secção A.16 e discriminação dos controlos avaliados

A secção A.16 destaca-se, por ser a secção com classificação mais baixa, encontrando-se abaixo do nível médio de maturidade, como é possível verificar na tabela 22.

O MTN não possui um documento formal que estabeleça as responsabilidades e os procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas em caso de incidentes de Segurança da Informação. Os procedimentos existem, mas não estão normalizados.

O facto de não existir um documento formal faz com que os controlos incluídos na secção sejam classificados maioritariamente com o nível 2, o que significa que os procedimentos são realizados de forma repetitiva e geralmente sempre pela mesma pessoa, mas não há um processo normalizado.

O primeiro passo para melhorar o nível de maturidade desta secção é a implementação de um procedimento documentado e de seguimento obrigatório, que estabeleça as responsabilidades e os procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas em caso de incidentes de Segurança da Informação, devendo para isso ser consideradas as seguintes diretrizes:

a) responsabilidades pela gestão devem ser estabelecidas para assegurar que os seguintes procedimentos são desenvolvidos e comunicados, de forma adequada, dentro da organização:
    1. procedimentos para preparação e planeamento a respostas a incidentes;

2. procedimentos para monitorização, deteção, análise e notificação de incidentes e eventos de Segurança da Informação;
3. procedimentos para registar as atividades de gestão de incidentes;
4. procedimentos para tratamento de evidências forenses;
5. procedimentos para avaliação e decisão dos eventos de Segurança da Informação e avaliação de fragilidades de Segurança da Informação;
6. procedimentos para resposta, incluindo os relativos à recuperação controlada de um incidente e comunicação a pessoas ou organizações relevantes, internas e externas.

b) procedimentos estabelecidos assegurem que:
   1. pessoal competente trata as questões relativas a incidentes de segurança dentro da organização;
   2. um ponto de contato para notificação e deteção de incidentes de segurança está implementado;
   3. contatos apropriados são mantidos com autoridades, grupos de interesses externos ou fóruns que tratam de questões relativas a incidentes de Segurança da Informação.

c) convém que procedimentos de notificação incluam:
   1. preparação de formulários de notificação de evento de Segurança da Informação para apoiar as ações de notificação e ajudar a pessoa a lembrar-se de todas as ações necessárias no caso de um evento de Segurança da Informação;
   2. o procedimento a ser realizado no caso de um evento de Segurança da Informação, por exemplo relatar todos os detalhes (tipo de não conformidade ou violação, mau funcionamento, mensagens no ecrã, comportamento estranho) imediatamente; e não tomar nenhuma atitude sozinho, notificar imediatamente ao ponto de contato, tomando apenas ações coordenadas;
   3. referência a um processo disciplinar formal estabelecido para tratar com funcionários que cometam violações de Segurança da Informação;
   4. processos de *feedback* adequados para assegurar que as pessoas que reportaram eventos de Segurança da Informação são informadas dos resultados depois de a questão ter sido tratada e encerrada.

Controlo	Descrição	Maturidade Média
A.17	**Aspetos da segurança da informação na gestão da continuidade do negócio**	**3,50**
A.17.1	**Continuidade da segurança da informação**	**3,00**
A.17.1.1	Continuidade da segurança da informação	
A.17.1.2	Implementação da continuidade da segurança da informação	
A.17.1.3	Verificar, analisar e avaliar a continuidade da segurança da informação	
A.17.2	**Redundâncias**	**4,00**
A.17.2.1	Disponibilidade dos recursos de processamento da informação	

Tabela 23: Avaliação da maturidade média da secção A.16 e discriminação dos controlos avaliados

A secção A.17, apresentada na tabela 23, tem como objetivo que a continuidade da Segurança da Informação seja considerada nos sistemas de gestão de continuidade do negócio da organização.

Verifica-se que o MTN tem presente a preocupação de não permitir a interrupção das atividades e proteger os processos críticos contra as consequências de falhas ou desastres significativos, tendo como objetivo o desenvolvimento contínuo de processos com vista à melhoria da proteção dos processos críticos face aos riscos existentes.

Recomenda-se, no entanto, que o MTN defina, documente, implemente e mantenha processos, procedimentos e controlos para assegurar o nível requerido de continuidade para a Segurança da Informação, durante uma situação adversa, devendo para isso assegurar-se que:

a) está implementada uma estrutura de gestão adequada para mitigar e responder a um evento de interrupção, usando pessoal com a necessária autoridade, experiência e competência;
b) o pessoal designado para dar resposta em caso de incidente tem a necessária responsabilidade, autoridade e competência para gerir um incidente e garantir a Segurança da Informação;
c) estejam desenvolvidos e aprovados planos documentados, procedimentos de recuperação e resposta, detalhando como a organização irá gerir um evento de interrupção e como manterá a sua Segurança da Informação num nível pré-determinado, com base nos objetivos de continuidade da Segurança da Informação aprovado pela direção (A.17.1.1).

Em função dos requisitos de continuidade de Segurança da Informação, convém que a organização estabeleça, documente, implemente e mantenha:

a) controlos de Segurança da Informação dentro dos processos de recuperação de desastre ou de continuidade do negócio, procedimentos e ferramentas e sistemas de suporte;
b) processos, procedimentos e mudança de implementação para manter os controlos de Segurança da Informação existentes durante uma situação adversa;
c) controlos compensatórios para os controlos de Segurança da Informação que não possam ser mantidos durante uma situação adversa.

Tendo em conta o controlo A.17.1.3 o MTN deverá ainda verificar, em intervalos regulares, se os controlos definidos e implementados para a continuidade da Segurança da Informação, continuam válidos e eficazes em situações adversas, devendo para isso:

a) testar e verificar a funcionalidade dos processos, procedimentos e controlos da continuidade da Segurança da Informação para garantir que são consistentes com os objetivos da continuidade da Segurança da Informação;
b) testar e verificar o conhecimento e rotina para operar os procedimentos, processos e controlos de continuidade da Segurança da Informação de modo a assegurar que o seu desempenho está consistente com os objetivos da continuidade da Segurança da Informação;
c) analisar criticamente a validade e eficácia dos controlos de continuidade da Segurança da Informação, relativos aos Sistemas de Informação, processos de Segurança da Informação, procedimentos e controles ou gestão da continuidade do negócio/gestão de recuperação de desastre e soluções de mudança.

Controlo	Descrição	Maturidade Média
A.18	**Conformidade**	**3,37**
A.18.1	**Cumprimento dos requisitos legais e contratuais**	**3,40**
A.18.1.1	Identificação da legislação aplicável a requisitos contratuais	
A.18.1.2	Direitos de propriedade intelectual	
A.18.1.3	Proteção de registos	
A.18.1.4	Proteção e privacidade de informações de identificação pessoal	
A.18.1.5	Regulamentação dos controlos criptográficos	
A.18.2	**Análise crítica da segurança da informação**	**3,33**
A.18.2.1	Análise independente da segurança da informação	
A.18.2.2	Cumprimento das políticas e normas de segurança	
A.18.2.3	Análise da conformidade técnica	

Tabela 24 - Avaliação da maturidade média da secção A.16 e discriminação dos controlos avaliados

O objetivo da secção A.18, apresentada na tabela 24, é evitar a violação de qualquer lei, estatuto, regulamento ou obrigação contratual relacionadas com a Segurança da Informação e de quaisquer requisitos de segurança.

Para garantir o cumprimento destes requisitos o MTN deverá efetuar a normalização dos processos referidos nas anteriores seções, de forma a que estes se tornem formalmente aceites e de seguimento obrigatório, evitando assim a violação de qualquer lei, estatuto, regulamento ou obrigação contratual relacionadas com a Segurança da Informação e de quaisquer requisitos de segurança.

6 Considerações Finais

6.1 Conclusões

Com a realização deste trabalho pode concluir-se que a utilização da ISO/IEC 27002:2013 combinada com um modelo de maturidade constituem uma boa ferramenta de autoavaliação da segurança de Sistemas de Informação.

A análise dos resultados obtidos, demonstram que o MTN possui um nível de maturidade médio geral de 3, o que significa que, em média, os seus procedimentos de segurança estão normalizados, documentados, são divulgados em formação e têm de ser seguidos obrigatoriamente. Os processos não são sofisticados, mas existe a formalização das práticas existentes. Existem procedimentos para melhorar e a segurança dos Sistemas de Informação deve ser aprofundada.

Tendo em conta os resultados obtidos deduz-se que o MTN, mais concretamente a DTICMA, na sua atividade tem presente a maioria das recomendações da ISO/IEC 27002:2013.

No entanto, apesar de os princípios e políticas inerentes à ISO/IEC 27002:2013 serem uma preocupação, verifica-se a falta de normalização de alguns processos, de forma a que estes se tornem formalmente aceites de seguimento obrigatório e divulgados em formação.

A utilização de uma escala de maturidade permitiu de forma simples e direta identificar as áreas que estão abaixo da média (áreas críticas) e que necessitam de melhoria, são elas, A.8 – Gestão de ativos (2,83), A.15 Relação com fornecedores (2,58) e A.16 Gestão de incidentes de Segurança da Informação (2,14).

A classificação abaixo da média nestas secções deve-se fundamentalmente ao facto de não existirem procedimentos documentados nestas áreas. Apesar de existir uma preocupação e serem realizados procedimentos, não havendo um procedimento documentado, que seja de seguimento obrigatório, é provável que ocorram falhas.

A existência de procedimentos normalizados é de extrema importância pois permite uma rápida deteção de falhas e imediata correção.

Os processos informais, por sua vez, dão lugar a que nem sempre sejam aplicados, pois não são obrigatórios nem existe um procedimento especifico a seguir, podendo também ocorrer que, para a mesma tarefa, dois funcionários executem procedimentos diferentes, por uma ordem diferente e/ou sem o mesmo rigor, podendo originar vulnerabilidades que podem ser exploradas por ameaças especificas.

A identificação direta das áreas mais críticas não era até aqui possível, pois o MTN não possuía um método de avaliação dos controlos de segurança do Sistema de Informação. A utilização deste método de avaliação proporciona uma visão abrangente de todo o Sistema de Informação, permitindo perceber se os controlos utilizados são os mais adequados e quais necessitam de ser melhorados.

A aplicação, de forma periódica, desta ferramenta permite a melhoria continua dos processos de segurança de informação através da identificação da necessidade de ajustamentos, sempre com o objetivo de melhorar a sua eficiência e eficácia e elevar o grau de maturidade dos Sistemas de Informação do Município.

Os resultados obtidos com esta avaliação podem também ser utilizados como suporte para a tomada de decisões relacionadas com melhorias e investimento necessários para assegurar a Segurança da Informação, bem essencial do Município.

6.2 Trabalhos Futuros

Relativamente a trabalhos futuros, seria pertinente utilizar a ISO/IEC 27002:2013 em conjunto com o modelo de maturidade para avaliar outros municípios, podendo assim ser efetuadas comparações e perceber como a gestão da segurança de Sistemas de Informação está a ser efetuada neste tipo de organizações em Portugal.

Tendo em conta a Lei Geral de Proteção de Dados (LGPD), seria também interessante, implementar em paralelo, a norma ISO 27701 – Sistema de Gestão de Segurança Privada, que tem como objetivo adicionar controlos no sistema de gestão para garantir a total privacidade especificamente dos dados pessoais.

Referências Bibliográficas

AIRC. *As Aplicações do ERP AIRC*. Obtido em 19 de janeiro de 2021, de http://www.airc.pt/produtos/erp-airc

AIRC. (s.d.). Gestão Documental e de Processos - Soluções de Gestão Documental e de Processos para a Administração Pública. *Documento de apoio a formação*.

Almeida, J. F., & Pinto, J. M. (1995). *A Investigação nas Ciências Sociais.* Lisboa: Editorial Presença.

Barbosa, A. M. (2012). *A Relação e a Comunicação Interpessoais entre o Supervisor Pedagógico e o Aluno Estagiário - Um Estudo de Caso.* Projeto de Mestrado. Lisboa: Escola Superior de Educação João de Deus.

Beal, A. (2005). *Segurança da Informação: Principios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações.* São Paulo: Atlas.

Beal, A. (2008). *Segurança da informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações* (1ª edição - 2ª reimpressão ed.). São Paulo: Atlas.

Borges, A., Rodrigues, J. A., & Rodrigues, R. (2010). *Elementos de Contabilidade Geral* (25.ª edição ed.). Lisboa: Áreas Editora.

Caixeiro, C. M. (2014). *Liderança e Cultura Organizacional: o Impacto da Liderança do Diretor na(s) Cultura(s) Organizacional(ais) Escolar(es).* Tese de Doutoramento. Évora: Universidade de Évora.

Cardoso, J. (2014). Sistemas de Informação para a Modernização Administrativa. *11.º Encontro Nacional de Arquivos Municipais.* Obtido em 20 de outubro de 2020, de https://www.bad.pt/publicacoes/index.php/arquivosmunicipais/article/view/1161/1154

Carneiro, A. (2002). *Introdução à Segurança dos Sistemas de Informação.* Lisboa: FCA.

Carvalho, C. M. (2018). *Segurança e Auditoria em Sistemas de Informação e Comunicação - Implementação numa Entidade Pública.* Projeto de Mestrado. Funchal: Universidade da Madeira.

Câmara Municipal de Torres Novas. *História*. Obtido em 15 de janeiro de 2021 de: https://www.cm-torresnovas.pt/index.php/historia

Côrte, K. (2014). *Segurança da Informação Baseada no Valor da Informação e nos Pilares Tecnologia, Pessoas e Processos.* Tese de Doutoramento. Brasília: Universidade de Brasília.

Costa, C. B. (1998). *Auditoria Financeira: Teoria e Prática* (6.ª edição ed.). Lisboa: Rei dos Livros.

Coutinho, C. P. (2006). Aspectos Metodológicos da Investigação em Tecnologia Educativa em Portugal (1985-2000). *14.º Colóquio da Secção Portuguesa da Association Francophone Internationale de Recherche Scientifique en Education (AFIRSE).* Lisboa. Obtido em 26 de dezembro de 2019, de http://hdl.handle.net/1822/6497

Coutinho, C. P., & Chaves, J. H. (2002). O Estudo de Caso na Investigação em Tecnologia Educativa em Portugal. *Revista Portuguesa de Educação*, 221-243. Obtido em 02 de janeiro de 2020, de http://hdl.handle.net/1822/492

Despacho n.º 8175/2020. (21 de agosto de 2020). *Regulamento de Organização dos Serviços Municipais, Afetação dos trabalhadores da Autarquia e Organograma*. Diário da República, 2.ª série, Parte H, N.º 163.

DGEEC, & DSECTSI. (2019). *IUTICCM 2018: Administração Pública Eletrónica 2018 - Câmara Municipais.* Obtido em 27 de outubro de 2020, de https://www.dgeec.mec.pt/np4/12.html

DGEEC, & DSECTSI. (2020a). *IUTICAP e IUTICCM 2019 - Segurança das TIC (cibersegurança) na Administração Pública Central, Regional e Câmaras Municipais.* Obtido em 27 de outubro de 2020, de https://www.dgeec.mec.pt/np4/%7B$clientServletPath%7D/?newsId=12&fileName=IUTIC2019_Ciberseguranca.pdf

DGEEC, & DSECTSI. (2020b). *IUTICAP e IUTICCM 2019 - Transformação Digital na Administração Pública Central, Regional e Câmaras Municipais.* Obtido em 27 de 10 de outubro 2020, de https://www.dgeec.mec.pt/np4/%7B$clientServletPath%7D/?newsId=12&fileName=IUTIC2019_TransformacaoDigital.pdf

Erickson, F. (1986). *Qualitative Methods in Research on Teaching.* New York: MacMilan.

Frisch, A. (2002). *Essential System Administration* (3.ª Edição ed.). USA: O'Reilly Media, Inc,.

Gouveia, L. B. (2004). *Local E-Government - A Governação Digital na Autarquia.* Porto: SPI - Sociedade Portuguesa de Inovação.

Gouveia, L. B., & Ranito, J. (2004). *Sistemas de Informação de Apoio à Gestão.* Porto: SPI - Sociedade Portuguesa de Inovação.

Guedes, V. L. (2010). *Controlo Interno - Impacto das Tecnologias de Informação nos Municipios.* Dissertação de mestrado. Aveiro: Universidade de Aveiro, Instituto Superior de Contabilidade e Administração.

Guttman, B., & Roback, E. A. (1995). *An Introduction to Computer Security: The NIST Handbook.* Washington: NIST, National Institute of Standars and Techonology.

ISO/IEC 27000:2018. (2018). ISO/IEC 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.

ISO/IEC 27002:2013. (2013). ISO/IEC 27002 - Information Technology - Security Techniques - Code of Pratice for Information Security - Controls. Standardization, International Organization for Standardization.

Laureano, M. A. (2005). Gestão de segurança da Informação. Obtido de https://www.slideshare.net/thiagoalvarenga752/apostila-itl-segurana-da-informao

Lifeapps. (15 de 10 de 2020). *Como o UX design está revolucionando o mercado digital*. Obtido de lifeapps: https://lifeapps.com.br/ux-design/

Lima, J. Á. (2006). Ética na Investigação. Em J. Á. Lima, & J. A. Pacheco, *Fazer investigação: Contributos para a elaboração de dissertações e teses.* Porto: Porto Editora.

Lima, M. S. (2016). *Capability Maturity Model Integration - CMMI.*

Lopes, I. M. (2012). *Adopção de Políticas de segurança de Sistemas de Informação na Administração Pública Local em Portugal.* Tese de Doutoramento. Minho: Universidade do Minho.

Marques, D. A. (2013). *Implementação de um Sistema de Controlo Interno numa Escola de Ensino Profissional.* Dissertação de Mestrado. Tomar: Instituto Politécnico de Tomar, Escola Superior de Gestão.

Marques, M. (1997). *Auditoria e Gestão.* Lisboa: Editorial Presença.

Marques, P. M. (abril_junho de 2016). Técnicas de Análise de Dados (Data Analytics) no Contexto de uma Auditoria Financeira (Parte I). *Revisores e Auditores, n.º 73*, pp. 12-23.

O'Brien, J. A., & Marakas, G. M. (2007). *Administração de Sistemas de Informação* (Tradução da 13ª ed.). New York: McGraw Hill.

Oliveira, J. A. (2005). *Abordagem Metodológica à Auditoria a Sistemas de Informação*. (IGF, Editor) Obtido em 08 de outubro de 2020, de https://www.igf.gov.pt/inftecnica/75_anos_IGF/oliveira/Oliveira_tema.htm

Pedro, J. M. (2010). *Livro Comemorativo dos 80 Anos da IGF-Autoridade de Auditoria - Sinais de inovação nas metodologias de controlo - Standards internacionais relacionados com o controlo interno na prespectiva dos sistemas de informção* (1.ª ed.). Lisboa: Edição da I. G. Finanças.

Pinheiro, J. M. (dezembro de 2007). Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. *Cadernos UniFOA*, pp. 11-21.

Pinheiro, P. P., & Sleiman, C. M. (2009). *Tudo o que você precisa saber sobre direito digital no dia-a-dia.* São Paulo: Saraiva.

Pinto, F. T. (2011). *Auditoria Contínua: Um novo Paradigma de Auditoria.* Provas de Título de Especialista, Instituto Politécnico do Porto, Escola Superior de

Tecnologias e Gestão de Felgueiras. Obtido em 20 de outubro de 2020, de https://core.ac.uk/download/pdf/47139827.pdf

Quivy, R., & Campenhoudt, L. V. (1998). *Manual de Investigação em Ciências Sociais* (2.ª ed.). (J. M. Marques, M. A. Mendes, & M. Carvalho, Trads.) Lisboa: Gradiva.

Sêmola, M. (2014). *Gestão da Segurança da Informação: Visão Executiva* (2.ª Edição ed.). Rio de Janeiro: Elsevier.

Silva, L. F. (2010). *Gestão de Riscos em Tecnologia da Informação como Fator Crítico de Sucesso na Gestão da Segurança da Informação dos Órgãos da Administração Pública Federal: Estudo de Caso da Empresa Brasileira de Correios e Telégrafos - ECT.* Dissertação de Mestrado. Brasília: Universidade de Brasília.

Silva, P. T., Torres, C. B., & Carvalho, H. (2003). *Segurança dos Sistemas de Informação.* V. N. de Famalicão: Edições Centro Atlântico.

Sousa, M. A. (2013). *Levantamento e Avaliação do Controlo Interno de uma Empresa do Ramo Alimentar.* Projeto de Mestre. Tomar: Instituto Politécnico de Tomar, Escola Superior de Gestão.

Trigacheiro, C. F. (2012). *O Impacto das Tecnologias de Informação na Avaliação dos Sistemas de Controlo Interno das Organizações.* Tomar: Instituto Politécnico de Tomar, Escola Superior de Gestão.

Vidigal, L. (1992). A Informática na Administração Pública: Contributos para um Retrato. *Informação e Informática - Revista do Instituto de Informática, Ministério das Finanças*.

Vidigal, L. (2013). A Reforma da Administração Pública à Luz dos Sistemas de Informação. *13.º Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI'2013).* Obtido em 20 de outubro de 2020, de http://revista.apsi.pt/index.php/capsi/article/download/43/38

Vieira, A. C. (2019). *Os Sistemas de Informação e a Eficiência da Auditoria.* Dissertação de Mestrado. Porto: Politécnico do Porto, Instituto Superior de Contabilidade e Administração do Porto.

Wadlow, T. A. (2000). *Segurança em Redes.* Rio de Janeiro: Campus.

Yin, R. K. (2010). *Estudo de Caso: Planejamento e Métodos* (4.ª ed.). (A. Thorell, Trad.). São Paulo: Bookman.

Anexos

Anexo 1

Despacho n.º 8175/2020

Artigo 8.º

Atribuições e Competências da Divisão de Tecnologias de Informação, Comunicação e Modernização Administrativa

No âmbito das áreas de informática e tecnologias de informação:

***a*)** Projetar, configurar e administrar os equipamentos e sistemas informáticos do município, nomeadamente os componentes de hardware, servidores, sistemas de informação, bases de dados e aplicações, incluindo os seus sistemas de proteção, segurança e controlo de acesso e infraestruturas de comunicação de dados ou voz, garantindo a sua adequada interligação a todas as estruturas funcionais e serviços municipais e assegurando a respetiva manutenção, atualização e correta operacionalidade;

***b*)** Definir, projetar e implementar planos estratégicos de promoção da inovação tecnológica e modernização administrativa, para a melhoria da qualidade e eficácia dos serviços municipais e a adoção de medidas e iniciativas de e -government que, em conjunto, permitam alcançar os objetivos estratégicos definidos;

***c*)** Dinamizar e potenciar a informatização através da realização de projetos de Investigação e Desenvolvimento (I&D) que visem a avaliação das novas tecnologias e o benefício na sua utilização, identificando os equipamentos os sistemas ou as infraestruturas tecnológicas cuja adoção represente uma mais -valia adequada às necessidades identificadas pelos órgãos e serviços municipais;

***d*)** Supervisionar e assegurar o cumprimento do Regulamento Interno de Informática, contribuindo para uma melhor utilização e gestão dos recursos e dos serviços informáticos existentes, com vista a uma eficiente utilização dos mesmos e à salvaguarda da sua segurança, integridade e correto funcionamento;

***e*)** Promover a conceção, o acompanhamento e a adoção de medidas e projetos de desmaterialização, agilização de processos e simplificação de circuitos, com objetivos de redução de custos e aumento da eficiência, garantindo ainda a sua adequada integração nos sistemas de informação municipal e de gestão da qualidade;

***f*)** Supervisionar, acompanhar e emitir parecer técnico sobre processos de aquisição ou seleção de equipamentos, aplicações ou sistemas informáticos, assegurando o cumprimento dos requisitos técnicos e funcionais adequados e pretendidos;

***g*)** Assegurar o apoio e suporte aos diversos serviços municipais e aos utilizadores no manuseamento de sistemas e equipamentos informáticos, potenciando a correta e eficiente utilização dos mesmos, através de acompanhamento direto ou recorrendo a ferramentas informáticas, metodologias formativas ou à elaboração de manuais e documentação de apoio;

***h*)** Acompanhar o desenvolvimento de obras e projetos municipais que incluam componentes tecnológicos, em especial os que impliquem aquisição, montagem ou adoção de soluções de hardware, software, processos informatizados, equipamentos ou outros sistemas informáticos, de forma a garantir a sua adequação técnica às infraestruturas existentes e a correta resposta às definições do projeto informático municipal;

***i*)** Dinamizar e acompanhar projetos que promovam a utilização de tecnologias de informação e comunicação junto dos munícipes e da população em geral, nomeadamente através de ações de sensibilização e apoio, ou pela disponibilização de informações e serviços ao cidadão, recorrendo a plataformas eletrónicas, às novas tecnologias e às redes de comunicações em particular à internet.

ipt.pt