TÉCNICO LISBOA

Análise ao Quadro Nacional de Referência de Cibersegurança

Implementação no QNRCS em PMEs

João Halm Gomes da Costa

Dissertação para obtenção do Grau de Mestre em

Mestrado de Segurança de Informação e Direito no Ciberespaço

Orientador: Pedro Adão

Jurí

Presidente: Carlos Caleiro

Orientador: Pedro Adão

Vogal: Miguel Mira da Silva

Dezembro 2021

Agradecimentos

Esta tese foi, em si, um processo de melhoria constante. Numa época em que os avanços tecnológicos e a sua relação com o mercado evoluem a um ritmo mais rápido do que usualmente dissertações deste género conseguem acompanhar, a consulta de vários profissionais da área de segurança de informação foi essencial para se concluir este trabalho académico.

Sendo esta dissertação o sinónimo de conclusão do Mestrado de Segurança de Informação e Direito no Ciberespaço, devo uma palavra de agradecimento aos meus colegas do curso do ano 2016/2017, e aos meus colegas de trabalho, em especial ao Bruno Miguel.

Por fim, um agradecimento muito especial à minha família e em especial ao meu pai por me ter encorajado a efetuar este mestrado.

Resumo

Esta dissertação de mestrado MSIDC do Instituto Superior Técnico, propõe a implementação do quadro de segurança português QNRCS - Quadro Nacional de Referência para a Cibersegurança nas PME. Esta implementação segue passo a passo os pontos de ação do *framework*, identificando lacunas no caminho e propondo soluções baseadas numa metodologia de abordagem ao risco.

Conteúdo

Índice de imagens

Índice de tabelas

Glossário

TERMO	DEFINIÇÃO
Ameaça	Potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização.
Confidencialidade	A propriedade de a informação não ser divulgada a pessoas ou entidades não autorizadas, ou segundo processos não autorizados.
Continuidade do negócio	Capacidade da organização para continuar a fornecer produtos ou serviços a níveis aceitáveis pré-definidos, na sequência de um incidente disruptivo.
CNCS	Centro Nacional de Cibersegurança
Disponibilidade	Propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada.
Framework	Modelo de referência.
Integração Contínua	Prática de engenharia de software que promove a consolidação de código numa cadência curta, tipicamente diária, tendo por objetivo simplificar o processo de integração das várias peças produzidas.
Integridade	A propriedade de salvaguardar o caráter exato e completo da informação e dos ativos.
Melhoria contínua	Atividade recorrente com vista a incrementar a capacidade para satisfazer requisitos.
Operador de infraestrutura crítica	Uma entidade pública ou privada que opera uma infraestrutura crítica.
Operador de serviços essenciais	Uma entidade pública ou privada que presta um serviço essencial
Plano da continuidade do negócio	Procedimentos documentados que orientam as organizações para responder, recuperar, retomar e restaurar um nível pré-definido de operacionalização, após disrupção.
Prestador de serviços digitais	Uma pessoa coletiva que presta um serviço digital.

Capítulo 1 - Introdução

1.1. O novo paradigma

Em 2007, a Estónia foi alvo de um ataque informático em larga escala, que paralisou todo o país [12]. Este país, outrora dentro da esfera soviética, atravessou uma profunda transformação tecnológica e económica desde a dissolução da União Soviética e, no processo subsequente de modernização, havia passado por uma transformação digital considerável, elevando o estatuto da nação báltica ao nível de pioneira no domínio do uso das tecnologias de informação em serviços do sector privado e do Estado. Contudo, apesar da modernização do país ter trazido claras melhorias na qualidade de vida do povo estónio, também o expôs a uma nova ameaça invisível que não podia ser combatida no mundo físico – ataques informáticos. Assim, a 26 de Abril de 2007, após a transladação de uma estátua simbólica do regime soviético de uma zona nobre de Talim para outra zona de menor valor simbólico, a Estónia foi alvo de um conjunto de ciberataques que duraram 3 dias.

Estes ataques materializaram-se sobre a forma de DDoS (Distributed Denial of Service) – que tiveram como objetivo sobrecarregar os sistemas informáticos com pedidos, ao ponto de os tornarem inoperacionais – e visaram as principais instituições do país. Com efeito, páginas web dos ministérios e serviços do Estado ficaram inoperacionais, tais como instituições bancárias e consequentemente todas as transações bancárias deixaram de funcionar. Tais ataques tiveram um efeito devastador na economia estónica, totalizando num prejuízo de milhões de euros e

Figura 1 - Norse Map

se, prejuízos esses para os quais não possível encontrar culpados.

Até então, episódios como este eram apenas contemplados em filmes de ficção científica e videojogos, mas o ataque às infraestruturas estónias serviu de chamada de atenção ao resto do mundo, na medida que nos mostrou, enquanto sociedades dependentes das tecnologias de informação, que estamos expostos a ameaças de natureza digital, cujos efeitos e consequências se podem materializar no mundo físico. Este acontecimento não foi isolado, pois as últimas duas décadas têm-nos dado mais exemplos (Stuxnet, Geórgia, etc…).
Mas se é verdade que a Internet é um novo cenário para campos de batalha entre Estados, é igualmente verdade que se tornou também palco para atividade criminosa, nomeadamente espionagem (política e industrial). A espionagem industrial é uma atividade que não é nova, mas os métodos pelos quais são efetuadas atividades de espionagem são-no. Estas atividades de espionagem podem ter um forte impacto na economia de um país, na medida em que um dos seus ativos mais valiosos – a tecnologia ou '*know how*' de ponta – pode ser utilizada por um adversário e desta forma, o país que é alvo de espionagem pode perder vantagem competitiva, sem ter a possibilidade de recuperar os elevados investimentos necessários para se alcançar esse nível tecnológico.

É importante ter em conta que este fenómeno não é esporádico, e que atualmente algumas nações são acusadas de fazer uso deste método para se industrializar, roubando informação sensível como modelos de negócio, tecnologia e outros ativos a nações mais industrializadas para depois vender internamente ao seu sector industrial. Por outro lado, muitos países têm demorado a reagir contra esta esta nova ameaça (de alcance global), e em resultado disso, o crime informático – que há 50 anos não existia – é um fenómeno em expansão. Mas, se o meio pelo qual a informação crítica dos nossos estados e das nossas empresas se encontra ameaçada é novidade e fruto de estudo em tempos modernos, a sua motivação é antiga. É por este motivo, que se alcunhou a temática da proteção de informação sensível de "Segurança de Informação" – e que atualmente várias organizações empregam políticas e medidas holísticas que visam a sua salvaguarda.

1.2. Já passámos por isto?

A segurança de informação sempre foi um fator determinante no sucesso de estratégias – sejam militares, comerciais ou outras. De facto, o conceito não é novo, tendo o mesmo estado sempre presente ao longo da história e sendo o seu tratado escrito mais antigo conhecido datado de 2500 anos (Arte da Guerra de Sun Tzu). Por cá, o velho ditado: "o segredo é a alma do negócio" é testemunha deste facto.

Apesar de não se saber ao certo a origem da expressão, a mesma reflete uma verdade incontornável. Pois se é verdade que o segredo é a chave de sucesso para qualquer empreendimento, também é verdade que a quebra do sigilo pode significar o fim de qualquer projeto. A História, e em particular a do nosso país, está repleta destes exemplos, mas talvez o

exemplo mais gritante esteja relacionado com a época dourada da história portuguesa, a epopeia os Descobrimentos.

Os Descobrimentos não foram fruto do acaso. O seu sucesso foi fruto de um projeto bem planeado (e reajustado) e executado de forma metódica e com uma abordagem científica. É bem conhecido o investimento da coroa portuguesa, o qual incluiu a contratação de mão de obra especializada - especialistas de navegação, matemáticos, engenheiros, cartógrafos - e empréstimos avolumados de dinheiro. Este esforço traduziu-se mais tarde em conhecimento (*know-how*), conhecimento este que seria a principal chave do sucesso do empreendimento português além-mares e alvo de cobiça das restantes nações europeias. Por este motivo, os mapas cartografados pelos navegadores lusos foram considerados como material secreto, e apenas um número seleto de pessoas tinham acesso a eles.

A hegemonia portuguesa no mar durou enquanto este *know-how* permaneceu somente na sua posse, mas a força da História viria a provar que seria apenas uma questão de tempo até as restantes potências europeias terem acesso à informação considerada 'Segredo de Estado' nacional (como o episódio do Planisfério de Cantino viria a demonstrar) e a rivalizar com Portugal nos mares e eventualmente retirando-lhe a hegemonia marítima, a qual o país nunca mais viria a recuperar. A economia nacional dessa época dependia fortemente do fenómeno dos Descobrimentos, que eram sobretudo potenciados pelo Estado; de facto os Descobrimentos constituíam praticamente um monopólio régio, no qual a restante economia assentava, ou seja, quase se pode dizer que o principal suporte do modelo de produção de riqueza nacional dependia do Estado.

Figura 2 - Planisfério de Cantino

Cinco séculos depois, o tecido económico afigura-se diferente. Atualmente, a produção de riqueza nacional jaz maioritariamente no sector privado. Este cenário descentralizado de produção de riqueza dificulta a coordenação de políticas de Segurança de Informação a nível nacional, pelo que tais medidas deverão ser levadas a cabo individualmente. Adicionalmente, e em virtude da globalização que expõe cada indivíduo a uma superfície de ameaça nunca antes

vista na história, este esforço coletivo de salvaguardar as informações críticas que suportam os sectores que contribuem para a produção de riqueza nacional torna-se ainda mais premente.
Mas não é apenas o risco de espionagem que há que temer, quando se aborda o tema da segurança de informação. Dezenas de ataques a bases de dados das organizações empresariais, estatais e outras, são periodicamente reportados nos meios de comunicação social. Regra geral estes ataques visam bloquear o acesso aos sistemas de informação das organizações, afetando com isso gravemente o funcionamento dessas entidades, exigindo os criminosos de seguida do pagamento de avultadas quantias para efetuarem o desbloqueamento. Acontece ainda que o desenvolvimento da tecnologia traz consigo, como sempre acontece, uma face positiva e uma face negativa. Os ataques aos sistemas de informação são cada dia mais sofisticados, obrigando a uma permanente atenção e esforço de atualização para os neutralizar. Malfeitores que se apropriam da possibilidade de acesso aos sistemas de informação de terceiros, para daí darem instruções lesivas para os interesses da vítima a outras entidades (ex: bancos), começam a ser frequentes hoje em dia.

1.3. Estamos preparados?

Em Portugal, a dependência das empresas e do Estado para com as tecnologias de informação e comunicação é cada vez mais uma realidade inegável e irreversível. Tal fenómeno é o resultado da transformação digital que o país tem atravessado, quer por iniciativa das próprias empresas para reduzir custos e melhorar processos e otimizar recursos, quer por iniciativa do Estado em encorajar tal transformação[1]. Dados de 2019 provenientes do INE mostram que quase um quinto do volume de negócios das empresas com 10 ou mais trabalhadores provem de comércio eletrónico. Valor este que conheceu um significativo aumento para 27% em 2020, devido em grande parte à pandemia que o país tem vivido (Covid.19)[2].

	Escalão de pessoal ao serviço	Computador	Internet	Website
2015	1 -9 pessoas	86,3%	77,9%	30,1%
	10 ou mais pessoas	99,2%	98,1%	61,5%
2019	1 -9 pessoas	95,6%	89,7%	30,2%
	10 ou mais pessoas	99,2%	98,3%	58,6%

Tabela 1 - Proporção de empresas que utilizam tecnologias da informação e da comunicação (%) por Escalão de pessoal ao serviço e Tipo de tecnologia (informação e comunicação) em 2018 e 2019 [5]

O quadro acima revela um significativo aumento na utilização de computadores e internet nas empresas até 9 colaboradores. Numa situação, mais ou menos estabilizada (com valores já perto to máximo) nas empresas com 10 ou mais pessoas no período entre 2015 e 2019.

[1] Em 2019, o Governo eleito criou a Secretaria de Estado da Transformação Digital, sob a tutela do Ministério da Economia [3].

[2] Segundo o estudo da Associação da Economia Digital [26]

Como já foi referido, a criminalidade informática é um fenómeno que não existia há 50 anos atrás e que tem crescido nos últimos anos. De acordo com o relatório de Anual de Segurança Interna de 2018 [7], é notória uma clara tendência crescente de criminalidade informática participada[3], apesar da ligeira diminuição de 2017 para 2018, sendo o "acesso/interceção ilegítima" o crime informático mais participado, seguido do crime de "sabotagem informática" e de "falsidade informática".

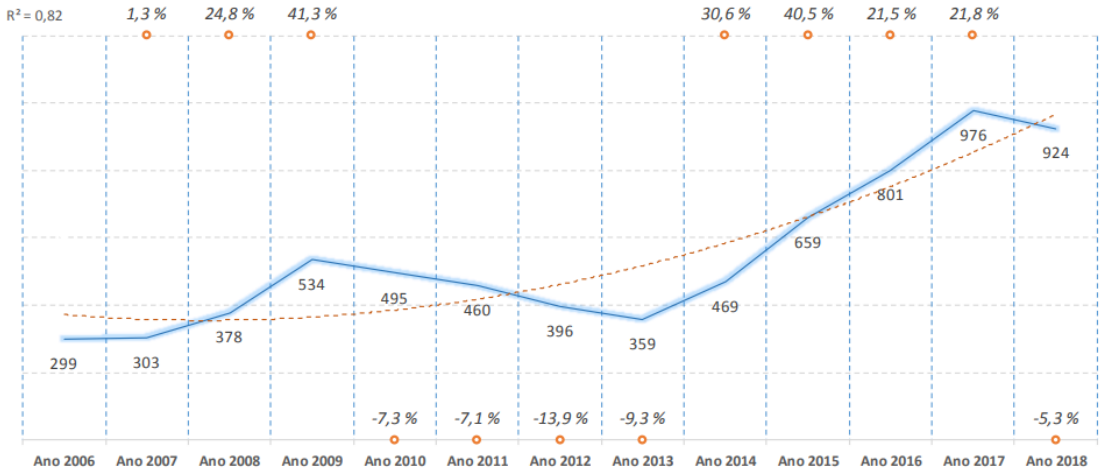


Figura 3 - Evolução dos crimes informáticos participados entre 2006 e 2019 [7]

Estes crimes, e especialmente os crimes de "acesso/interceção ilegítima", "sabotagem informática" e "falsidade informática", têm como principal vetor de ataque a técnica de *phishing*[4], cuja mitigação passa pelo investimento em formação de pessoal no correto manuseamento das tecnologias de informação. De acordo com os dados do INE, em Portugal em 2019, apenas 21% das empresas com 10 ou mais pessoas têm pessoal especialista em TIC.

[3] Para esta categoria foram consideradas as seguintes topologias: acesso indevido ou ilegítimo/interceção ilegítima; falsidade informática; outros crimes informáticos; reprodução ilegítima de programa protegido; sabotagem informática e viciação ou destruição de dados/ dano relativo a dados/programas.

[4] O Relatório de Cibersegurança em Portugal | Riscos & Conflitos de Maio de 2021 do CNCS [4] refere que o phishing/smishing e o sistema infetado por malware continuam a ser os tipos de incidentes mais registados pelo CERT.PT, em 2020, tal como no ano anterior.

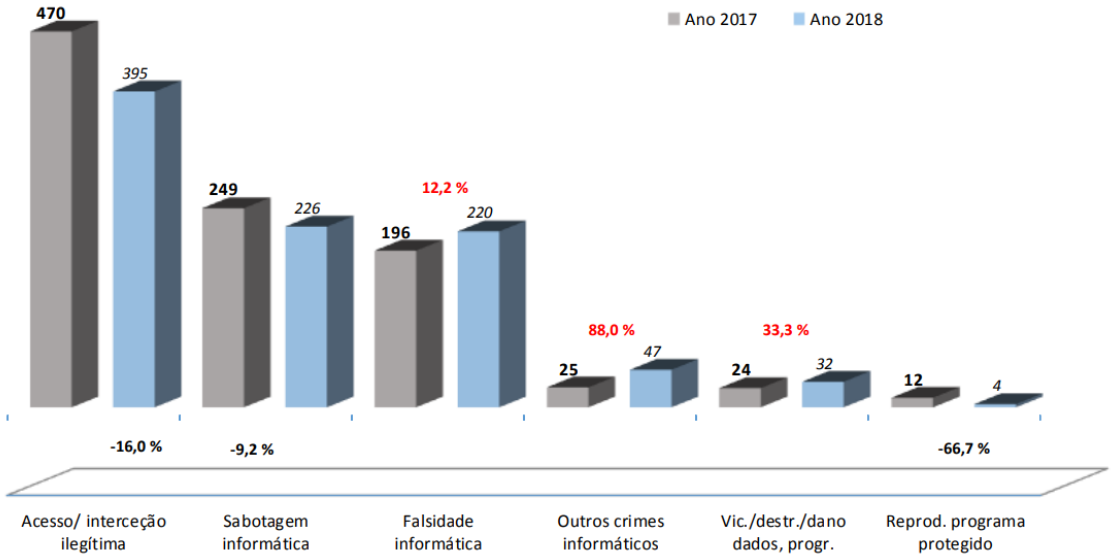


Figura 4 - Principais tipos de crime reportados entre 2017 e 2018 [7]

De acordo com o mesmo estudo, as ações de formação para desenvolver as competências em TIC promovidas pelas empresas (incluindo segurança) destinaram-se, sobretudo, a pessoal afeto a outras funções que não funções TIC. Em 2018, do conjunto de empresas com 10 ou mais pessoas que promoveram este tipo de formação, 11% referiu ter promovido ações de formação para especialistas em TIC e 25% para pessoal não especialista em TIC. Foram as grandes empresas que mais promoveram ações de formação em TIC, seja para especialistas (56%), seja para não especialistas (61%).

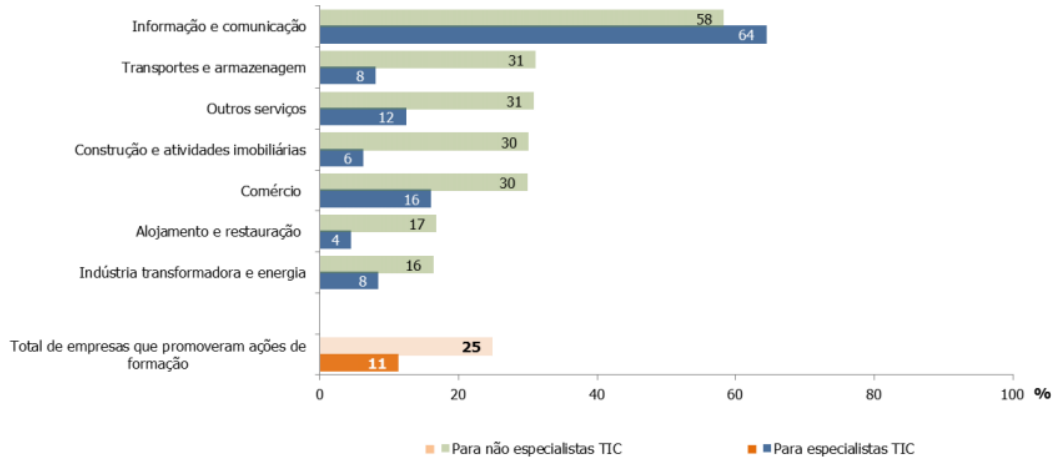


Figura 5 - Percentagem de empresas com 10 ou mais pessoas ao serviço que promoveram ações de formação em TIC, por setor de atividade económica (2018)

Assim, atendendo a que 45% do pessoal ao serviço de empresas utilizam computadores e que apenas 11% dos não especialistas em TIC têm ações de formação, podemos considerar um valor baixo de ações de formação face ao universo de pessoas que utilizam computadores (note-se que as ações de formação também devem englobar o uso de outros dispositivos, tais como telemóveis, cuja penetração ultrapassa a dos computadores em cerca de 71% para empresas com mais de 10 pessoas - e que também pode ser usado como canal de vetor de

ataque de *phishing*). Adicionalmente, em 2018, para as empresas com 10 ou mais pessoas ao serviço, a indisponibilidade de serviços foi o incidente de segurança relacionado com as TIC que mais ocorreu (24%). Os incidentes relativos à destruição ou corrupção de dados foram mencionados por 14% das empresas e 5% das empresas referiram incidentes relacionados com a divulgação de informação confidencial. Incidentes desta natureza podem originar avultados danos financeiros[5] e reputacionais nas empresas e em última instância, colocar a sua sobrevivência em causa.

Aliado a estes números preocupantes, acrescem os dados quantitativos relativos a fugas de informação à escala global: 4.1 biliões de registos roubados apenas na primeira metade de 2019, 52% das fugas de informação envolveram atividades de *hacking*, 28% envolveram o uso de *malware*, 32% incluíram *phishing* e 33% incluíram engenharia social.

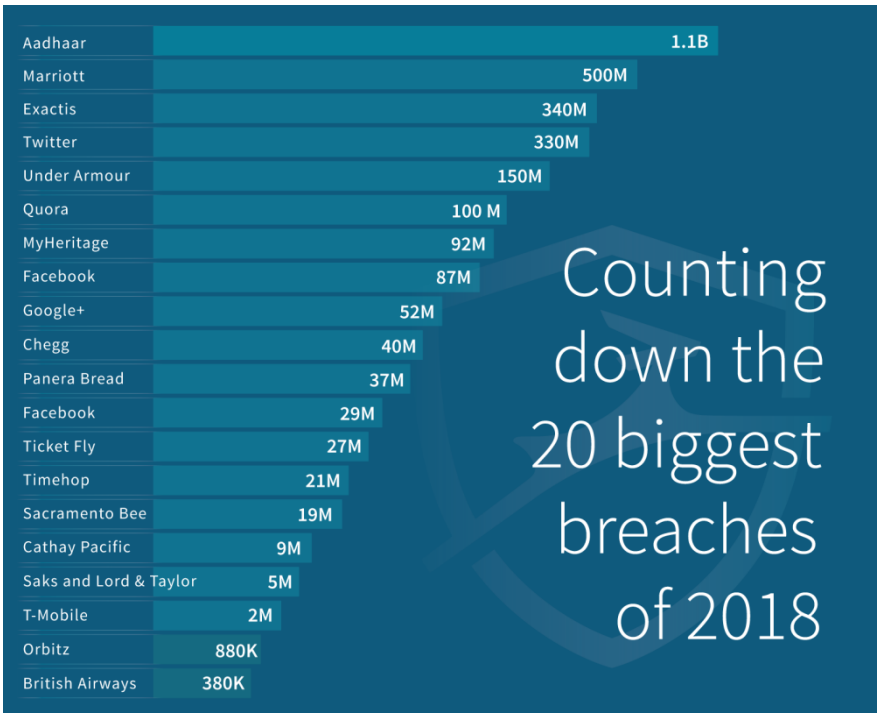


Figura 6- Lista de empresas vítimas de fugas de informação em 2018 (Dashlane) [10]

Estes e outros números preocupantes fizeram disparar o alarme entre as autoridades nacionais e europeias para o problema da cibersegurança e das fugas de informação. Assim, num esforço de fazer face aos novos desafios de segurança de informação colocados pela globalização e pela conjuntura geopolítica dela derivada, a União Europeia e Portugal em particular, tomaram várias medidas que visaram o aumento da resiliência da sociedade civil contra as ameaças de segurança externas e internas. Estas medidas materializam-se na elaboração de um conjunto de leis e regulamentos bem como na criação de organismos responsáveis pelo controlo desses mesmos regulamentos. É neste contexto que, de forma a facilitar a implementação de uma cultura de segurança de informação - nomeadamente de

[5] De acordo com a IBM, o valor médio do prejuízo proveniente de uma fuga de dados é de 3.92 milhões de dólares, sendo a Saúde o sector mais afetado [8]

cibersegurança - nos estados membros, a União Europeia criou a ENISA (*European Union Agency for Cyber Security*), que tem como finalidade criar sinergias entre os organismos competentes da cibersegurança dos vários estados membros, bem como ajuda-los no desenho e implementação de políticas de segurança entre outras atividades que envolvem a articulação dos vários organismos competentes para uma segurança mais eficiente.

Igualmente relevante, foi a contribuição da União Europeia - através do Parlamento Europeu - da promulgação de uma lei comum que estabelecia regras de tratamento de dados pessoais, as quais visam salvaguardar os direitos e liberdades individuais dos cidadãos europeus através do impedimento do uso abusivo dos seus dados pessoais - sobretudo digitais - por entidades terceiras. Esta lei viria a ser conhecida em Portugal por Regulamento Geral de Proteção de Dados - RGPD - e entrou em vigor em território nacional em 25 de Maio de 2018, sendo a sua fiscalização (e aconselhamento) levada a cabo em território nacional pela Comissão Nacional de Proteção de Dados (CNPD). A implementação do RGPD em Portugal não teve apenas um efeito meramente legal, já que o seu efeito psicológico teve um forte impacto no despertar do tema da Segurança de Informação na cultura nacional. De facto, as pesadas coimas associadas ao incumprimento das regras estabelecidas pelo RGPD fizeram soar vários alarmes no tecido empresarial português, que em grande parte - como veremos adiante - é constituído por pequenas e médias empresas e que, por conseguinte, é mais sensível a um impacto financeiro causado por esta coima do que uma grande empresa.

Figura 7 - Organizações criadas no âmbito da cibersegurança e segurança de informação

Entretanto, o Estado Português tomou as suas próprias medidas, conferindo deste modo um reforço às medidas tomadas por Bruxelas. Com efeito, algumas destas, como a Resolução do Conselho de Ministros 41/2018 ou a Resolução do Conselho de Ministros 46/2018, obrigam à

implementação de requisitos técnicos nos Sistema de Informação da Administração Pública e dos seus fornecedores privados (no caso de prestadores de serviços digitais) que têm como objetivo reforçar a segurança dos mesmos. Estes regulamentos, apesar de terem sido introduzidos em 2018, não estão sujeitos à mesma fiscalização que o RGPD, mas passaram a ser requisito praticamente obrigatório em todas as aquisições e implementações tecnológicas da Administração Pública, sendo as mesmas normalmente exigidas em concurso público.

Outra medida importante avançada pelo Estado Português foi a criação do Centro Nacional de Cibersegurança (CNCS). Trata-se de um organismo que "atua como coordenador operacional e autoridade nacional especialista em matéria de cibersegurança junto das entidades do Estado, operadores de infraestruturas críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais, garantindo que o ciberespaço é utilizado como espaço de liberdade, segurança e justiça, para proteção dos setores da sociedade que materializam a soberania nacional e o Estado de Direito Democrático." Com efeito, o CNCS não só tem tomado várias iniciativas de sensibilização para o tema da cibersegurança, como também tem promovido Regulamentos, que de momento não são vinculativos, entre outras medidas resultantes das sinergias criadas pelo organismo.

Finalmente, a criação da Rede Nacional CSIRT também constitui um forte contributo para a criação de uma rede nacional de resposta a incidentes de segurança, conferindo assim à sociedade civil um meio de resposta mais eficaz e de alerta a ameaças de cibersegurança à escala nacional. Esta rede é constituída por várias unidades CSIRT provenientes sobretudo do sector privado (mas não só) que são responsáveis pela monitorização e correlação de eventos de segurança nas suas organizações e dos seus clientes, que com base nos dados recolhidos permitem "criar indicadores e informação estatística nacional sobre incidentes de segurança com vista à melhor identificação de contramedidas pró-ativas e reativas" bem como "criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão".

A introdução de medidas de combate ao cibercrime e a implementação de regulamentos de cariz técnico relativamente ao uso da informação digital e de requisitos mínimos de segurança à infraestrutura de TIC das empresas é claramente uma medida necessária e importante, apesar de insuficiente. No entanto, estas medidas vão ganhando dia a dia mais relevo, e um exemplo disso é o surgimento cada vez mais regular de requisitos de cumprimento e de conformidade com estes regulamentos em cadernos de encargo de concursos públicos. Este exemplo é demonstrativo do fenómeno que, por via da necessidade, obrigará todas as empresas mais cedo ou mais tarde a cumprirem com estes regulamentos de segurança de informação, a fim de mantarem a sua atividade.

O cumprimento destes regulamentos obrigará inevitavelmente as empresas a investirem nas suas infraestruturas TIC, quer na aquisição de equipamento – software e hardware – quer no investimento em formação de pessoal. Tal poderá constituir um desafio ao crescimento ou

sobrevivência das micro e pequenas empresas e contribuir para o aumento do fosso de competitividade entre pequenas e grandes empresas. Assim, nasce a questão:

Terão as nossas micro e pequenas empresas capacidade de investimento nas TIC a fim de se manterem competitivas?

1.4. A motivação

De acordo com a entidade Pordata [9], as micro empresas compunham 96,2% do total de empresas em Portugal em 2017, sendo 3,2% consideradas pequenas empresas e 0,5% médias empresas.

Anos	Total	Micro Empresas	Pequenas Empresas	Médias empresas
2014	99,9	96,3	3,1	0,5
2015	99,9	96,2	3,2	0,5
2016	99,9	96,2	3,2	0,5
2017	99,9	96,2	3,2	0,5

Tabela 2 - Micro, Pequenas e médias empresas em % do total de empresas (INE)

Definição de Grande Empresa	• Empresas com 250 ou mais pessoas ao serviço ou; • Empresas com volume de negócios superior a 50 milhões de euros e ativo líquido superior a 43 milhões de euros • As empresas que não cumpriam estes critérios foram classificadas como PME, ou seja, pequenas e médias empresas.
Definição de Média Empresa	• Empresa que emprega menos de 250 pessoas e com; • Volume de negócios anual que não excede 50 milhões de euros ou balanço total anual não excede 43 milhões de euros, e que; • Não está classificada como micro ou pequena empresa.
Definição de Pequena Empresa	• Empresa que emprega menos de 50 pessoas e com • Volume de negócios anual ou balanço total anual que não excede 10 milhões de euros, e que; • não está classificada como uma microempresa.
Definição de Microempresa	• Empresa que emprega menos de 10 pessoas e cujo volume de negócios anual ou balanço total anual não excede 2 milhões de euros.

Tabela 3 -Definição de Grandes, Médias, Pequenas e Micro empresas [11]

Como se pode verificar na Tabela 3, as micro e pequenas empresas juntas constituíram 99,5% das empresas nacionais em 2017, o que é um grande número. Dada a magnitude destes números e o consequente peso destes na produção de riqueza nacional, é de esperar que qualquer obrigatoriedade no cumprimento destas normas de segurança represente um custo avolumado no orçamento de qualquer micro e pequena empresa. Por outro lado, o não cumprimento destas regras aumenta o risco de exposição a falhas de segurança, as quais se podem traduzir também em avolumados prejuízos.

Face a este dilema, a presente tese propõe-se a partir da aplicação a uma microempresa apresentar uma solução genérica de TI – arquitetura, aplicações e processos – orientada a pequenas organizações, que permita responder aos requisitos das normas em vigor em território nacional. De facto, as organizações de menor dimensão possuem menos recursos, quer humanos, quer tecnológicos, pelo que a todas as sugestões desta tese terão esse facto em mente. Para tal, serão sugeridas soluções *open source* sempre que disponíveis, em detrimento de soluções pagas.

Neste sentido, optou-se por recorrer ao Quadro Nacional de Referência para Cibersegurança como ponto de partida para esta análise. O QNRCS é um conjunto de recomendações de cibersegurança de origem portuguesa, que se baseia nas melhores práticas de normas de segurança de informação internacionais e nacionais[6], as quais serão aplicadas a uma PME. A tese fará uso de documentos de suporte ao QNRCS, e em caso de omissão, usará e justificará os seus pressupostos para a implementação da *framework* na organização. A esperança final é a que esta tese sirva como guia de implementação do QNRCS às PMEs.

1.5 Estrutura da dissertação

O objetivo desta tese é a demonstrar a implementação do QNRCS numa PME, e identificar os seus principais desafios. A título de análise, este trabalho académico apresentará uma implementação do Quadro numa microempresa, cuja metodologia poderá ser aplicada a qualquer PME.

Esta dissertação é constituída por 6 capítulos. No capítulo 2 – Revisão de Leitura, abordar-se-á o QNRCS tal como ele se encontra estruturado pelo CNCS e outros documentos de suporte ao QNRCS (ex: Quadro de Avaliação). Sendo que o objetivo da tese consiste em aplicar o QNRCS a uma micro organização à semelhança de uma *framework de segurança*, o capítulo 3 – Trabalho Empírico, estabelece os pressupostos para a execução da implementação (ex: gestão de risco, conformidade, entre outros). O capítulo 4 – Resultados, foca-se na aferição do estado "*as is*" do risco e dos controlos de segurança da organização[7] visada nesta tese, à luz das indicações do QNRCS e do Quadro de Avaliação, e das ações de ajuste das medidas de

[6] Como a RCM 41 / 2018 que visa estabelecer um regulamento para implementações técnicas a fim de fazer face aos desafios técnicos introduzidos pelo RGPD (Regulamento Geral de Proteção de Dados).

[7] Organização utilizada para testar a implementação do QNRCS.

segurança para com os níveis de exigência identificados à luz do Gestão de Risco. O capítulo 5 – Discussão, reflete sobre alguns pormenores também abordados no QNRCS e cruciais para o processo de gestão de segurança de informação e cibersegurança, como também sugere algumas implementações técnicas e processuais de segurança aplicáveis a qualquer PME. Por fim, o capítulo 6 traz à luz as conclusões do processo de implementação, refletindo acerca do seu impacto numa organização de pequena dimensão.

Capítulo 2 – Revisão de Leitura

2.1 A criação do QNRCS

O Quadro Nacional de Referência para a Cibersegurança, doravante denominado QNRCS, pretende ser uma ferramenta à disposição da sociedade para apoio a resposta sistemática à problemática da segurança. Em 2016, foi aprovada a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho, relativa a medidas destinadas a **garantir um elevado nível comum de segurança** das redes e dos sistemas de informação em toda a União (Diretiva SRI). Com a Diretiva SRI, pretendeu-se criar-se o enquadramento legal para a legislação dos Estados-Membros no domínio da cibersegurança e fornecer bases para desenvolver uma **cultura de cibersegurança** em setores vitais para a economia dos Estados-Membros e para o correto funcionamento da sociedade, setores esses que dependem fortemente das redes e sistemas de informação. Esta resposta está igualmente alinhada com a Lei n.º 46/2018, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva SRI.

Adicionalmente, o QNRCS dá cumprimento à Estratégia Nacional de Segurança do Ciberespaço, na sua versão atual, aprovada através da Resolução do Conselho de Ministros n.º 92/2019 de 23 de maio. **A Estratégia fundamenta-se no compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa do ciberespaço de interesse nacional e potenciar uma utilização livre, segura e eficiente do mesmo por parte de todos os cidadãos, das empresas e das demais entidades públicas e privadas.** A Estratégia alicerça-se em três princípios, os quais o QNRCS pretende endereçar da seguinte forma:

a) Subsidiariedade: o QNRCS pretende ser uma ferramenta transversal a todas as organizações intervenientes no ciberespaço, desde os operadores privados até ao Estado, enquanto responsável pelo garante da soberania e dos princípios constitucionais;
b) Complementaridade: sendo o QNRCS transversal, propõe um conjunto de medidas alargadas e integradoras que têm como objetivo potenciar a consciencialização entre todos os atores intervenientes no ciberespaço e a posição que ocupam no mesmo;
c) Proporcionalidade: no QNRCS, ao longo dos objetivos de segurança, propõe-se a adequação das medidas à organização, quanto à sua aplicabilidade, dimensão, setor de atividade e caraterização dos riscos identificados.

O QNRCS pretende ser aplicável, essencialmente, a organizações que assentem a sua atividade em tecnologia, quer seja numa perspetiva de cibersegurança para Tecnologias de Informação, de controlos de sistemas industriais, sistemas de interface homem-máquina, dispositivos IoT ou, de uma forma mais generalista, todos os dispositivos conectados de alguma forma a redes e sistemas de informação.

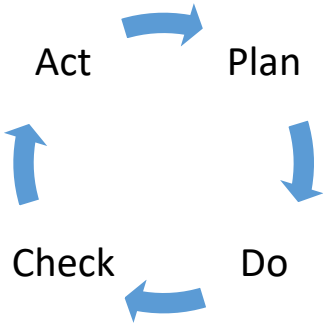


Figura 8 - PDCA

Á semelhança de sistemas de gestão, o QNRCS é uma norma que pretende sistematizar a abordagem à segurança, prezando pela melhoria contínua. O ciclo de vida do QNRCS assenta na avaliação sistemática do risco de cibersegurança.

2.2. Como se encontra estruturado

Está estruturado num conjunto de medidas de segurança que traduzem cinco objetivos específicos: Identificar, Proteger, Detetar, Responder e Recuperar.

- **Identificar** – Conhecer, num contexto organizacional, os recursos que suportam as suas funções importantes e os respetivos riscos associados, permite à organização priorizar os seus esforços de forma consistente.
- **Proteger** – Esta capacidade suporta-se, entre outras, na gestão da identidade eletrónica e respetivas autorizações, na realização de ações de formação e de sensibilização e na definição e implementação de procedimentos, processos e tecnologias de proteção da informação.
- **Detetar** – No contexto do objetivo "**Detetar**", pretende-se desenvolver práticas adequadas e atempadas à deteção da ocorrência de eventos de cibersegurança, por via da monitorização contínua das redes e sistemas de informação e da implementação de processos de deteção.
- **Responder** – Pretende-se, como resultado para o objetivo "**Responder"**, desenvolver e implementar práticas que levem a cabo ações de resposta a um incidente de cibersegurança que tenha sido detetado.
- **Recuperar** – No âmbito do objetivo "**Recuperar"**, pretende-se desenvolver e implementar práticas e manter planos de resiliência para restaurar qualquer capacidade e/ou serviço que tenha sido comprometido na sequência de um evento de cibersegurança.

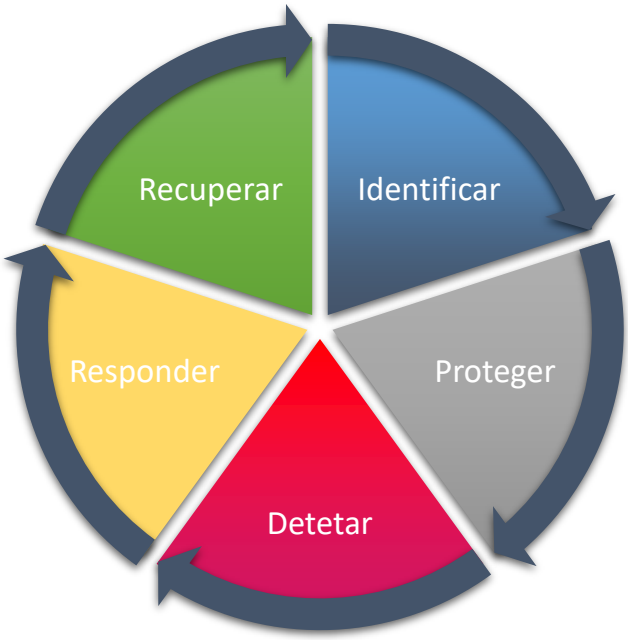


Figura 9 - Objetivos de Segurança

A estrutura central do QNRCS é constituída por:

1. Objetivos de segurança;
2. Medidas de segurança.

As medidas de segurança traduzem-se em categorias que se dividem em subcategorias. A cada objetivo de segurança, pode corresponder uma ou mais categorias. A cada categoria pode corresponder uma ou mais subcategorias.

A cada subcategoria está associado um ou mais controlos ou referências. O objetivo passa por interligar cada uma das subcategorias a referenciais de boas práticas de segurança da informação e de cibersegurança, por intermédio de um conjunto de práticas de referência e de maior aceitação/popularidade em Portugal.

Para cada subcategoria, referencia-se um exemplo de implementação tecnológica e outro de implementação processual, consistindo numa descrição genérica de como pode ser aplicado, contribuindo, desse modo, para uma melhor compreensão da aplicabilidade do mesmo. São ainda referenciados exemplos genéricos de possíveis evidências que podem ser utilizadas na demonstração da aplicação de determinada medida de segurança.

A estrutura base do QNRCS apresenta-se, assim, da seguinte forma:

OBJETIVO	MEDIDAS DE SEGURANÇA					
IDENTIFICAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
PROTEGER	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
DETETAR	Categorias	Subcategorias	Implementação	Implementação	Evidências	Referências

			Técnica	Processual		Normativas
RESPONDER	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
RECUPERAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas

Tabela 4 - Estrutura do QNRCS

São referenciados exemplos e orientações que permitem sistematizar processos e procedimentos cuja aplicação conduza ao cumprimento desses mesmos objetivos, não na forma de uma lista de controlo de ações a realizar, mas antes na representação dos objetivos chave reconhecidos pelos diversos intervenientes como uma referência de alto nível, assente num conjunto de referenciais internacionais e em diferentes normas técnicas.

- **CIS CSC 7.0 -** O Catálogo de controlos críticos de cibersegurança (CSC) é publicado pelo *Center for Internet Security* (CIS). Este catálogo disponibiliza uma lista de ações, priorizada, que é regularmente revista pela comunidade académica, de forma a ser utilizável pelas organizações.
- **COBIT 5 -** Da responsabilidade do ISACA [12], o COBIT é uma *framework* de boas práticas para governo de TI. Ajuda as organizações a criar valor a partir das TI e contribui para o equilíbrio entre os benefícios, a otimização dos níveis do risco e a utilização dos recursos disponíveis pelas organizações.
- **ISO/IEC 27001:2013 -** A norma ISO/IEC 27001 [13] especifica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação, bem como os requisitos para os controlos de segurança a serem implementados, de acordo com as necessidades e realidade da organização.
- **NIST SP-800-53 Rev4 -** Publicado pela NIST [14], é um catálogo de controlos de segurança e de privacidade para redes e sistemas de informação de organismos do governo. Disponibiliza, também, um processo de seleção de controlos para proteção da operação e dos ativos das organizações, de incidentes, desastres naturais, falhas estruturais ou erro humano.

Note-se que o QNRCS é mais orientado à cibersegurança do que à segurança de informação em geral (em oposição à ISO 27001) e foca-se sobretudo na resposta a incidentes de segurança de informação e cibersegurança em particular.

No âmbito da construção da estrutura central do QNRCS, são definidas todas as categorias, subcategorias e controlos/referências que se entendem relevantes, atendendo (mas não apenas) aos seguintes princípios:

a) considerar todos os aspetos definidores de um ecossistema de cibersegurança nas organizações nacionais, independentemente da sua dimensão, natureza (pública ou privada), criticidade ou orientação tecnológica;

b) abranger transversalmente todos os sectores de atividade;

c) atender às características específicas e definidoras do tecido social e económico do país;

d) permitir e promover que determinadas organizações (por exemplo: reguladores) possam definir o respetivo contexto de aplicação do QNRCS para o seu sector de atividade/regulação.

2.3 O Quadro de Avaliação das Capacidades Mínimas de Cibersegurança

O Quadro de Avaliação das Capacidades Mínimas de Cibersegurança é um produto complementar ao Quadro Nacional de Referência para a Cibersegurança (QNRCS), dando seguimento à estratégia do Centro Nacional de Cibersegurança (CNCS) para o suporte das organizações à sua capacitação, através da disponibilização de referenciais e ferramentas. Como complemento ao QNRCS apresenta, para cada uma das medidas de cibersegurança, a definição de três níveis de capacidade para que seja possível às organizações o cumprimento dos cinco objetivos do quadro, tendo em conta o seu contexto e dimensão.

Propõe-se a aplicação cumulativa das medidas definidas, ou seja, para que uma organização esteja posicionada no nível de capacidade "3 – Avançado", terá de implementar as medidas de nível "1 – Inicial[8]" e "2 – Intermédio".

As medidas de segurança têm os seus níveis de sofisticação distribuídos conforme a classificação apresentada e estão organizadas conforme a estrutura proposta de objetivos de segurança, descritos no QNRCS.

2.4 Metodologia

Os níveis de capacidade podem ser aplicados de forma independente a cada objetivo. Como resultado, uma organização pode posicionar-se em níveis de capacidade distintos para um mesmo objetivo de segurança. Os níveis de capacidade aplicáveis a uma determinada organização dependem das suas características específicas, tais como dimensão e serviços fornecidos. Sabendo que as organizações se podem encontrar em diferentes níveis de maturidade e possuir diferentes dimensões (desde micro e pequenas organizações a grandes empresas ou instituições públicas), e que algumas recomendações podem ser desproporcionalmente exigentes para a dimensão da organização ou não ser suficientemente exigentes, sugere-se que o documento seja interiorizado com espírito crítico por cada organização e adequado às suas necessidades.

Por este motivo, é recomendado à organização que implementa o QNRCS, que adeque a sua proporcionalidade à sua análise de Risco de Segurança de Informação, pelo que para tal, será necessário que a organização articule a implementação dos seus controlos com o processo de

[8] Nesta tese, este grau será doravante designado por grau 'Básico'.

Gestão de Risco de Segurança de Informação. Esta estratégia visa aproximar-se do processo de Gestão de Segurança de Informação preconizado pela norma ISO/IEC 27001. Não havendo um critério definido, sobre qual o grau de maturidade que a organização deverá apontar a sua implementação do QNRCS, o mesmo é estabelecido pela organização em causa.

A metodologia usada nesta tese segue o conjunto de passos recomendados do QNRCS. Estes passos permitem a sistematização e melhoria contínua de processos, e são:

- **Passo 1** – Prioridade e âmbito: A organização identifica os seus objetivos e prioridades de alto nível. Com esta informação, a organização define as suas opções estratégicas no que se refere à implementação de medidas de cibersegurança e define qual o universo de sistemas e ativos que suportam a atividade crítica da organização.
- **Passo 2** – Linhas orientadoras: uma vez definido o âmbito do programa de cibersegurança, a organização identifica e define as redes e sistemas de informação e respetivos ativos relacionados com a atividade, requisitos regulatórios e a estratégia de gestão do risco.
- **Passo 3** – Criação do Perfil Atual: A organização cria aquele que é o seu "Perfil Atual", indicando para cada categoria e subcategoria quais os objetivos de segurança que cumpre atualmente.
- **Passo 4** – Aferição do risco: A Análise do risco pode ser guiada de acordo com o processo de gestão do risco em vigor na organização, ou tendo por base ações anteriores. A organização analisa o seu ambiente operacional para aferir o grau de probabilidade de ocorrência de um evento ou incidente de cibersegurança e o impacto que este possa ter na organização.
- **Passo 5** – Criação do Perfil Alvo: A organização cria o seu "Perfil Alvo" com base nas categorias e subcategorias descritas no QNRCS, refletindo aqueles que são os resultados pretendidos.
- **Passo 6** – Identificar, analisar e priorizar lacunas: A organização compara o "Perfil Atual" com o "Perfil Alvo" e identifica lacunas que devem ser endereçadas.
- **Passo 7** – Implementação do plano de ação: A organização determina quais as ações a levar a cabo por forma a endereçar as lacunas identificadas no passo anterior e ajusta as práticas de cibersegurança que tenha atualmente em vigor, de modo a atingir o seu "Perfil Alvo".

As organizações devem repetir este processo sempre que necessário e, inclusivamente, com uma cadência projetada e sistematizada.

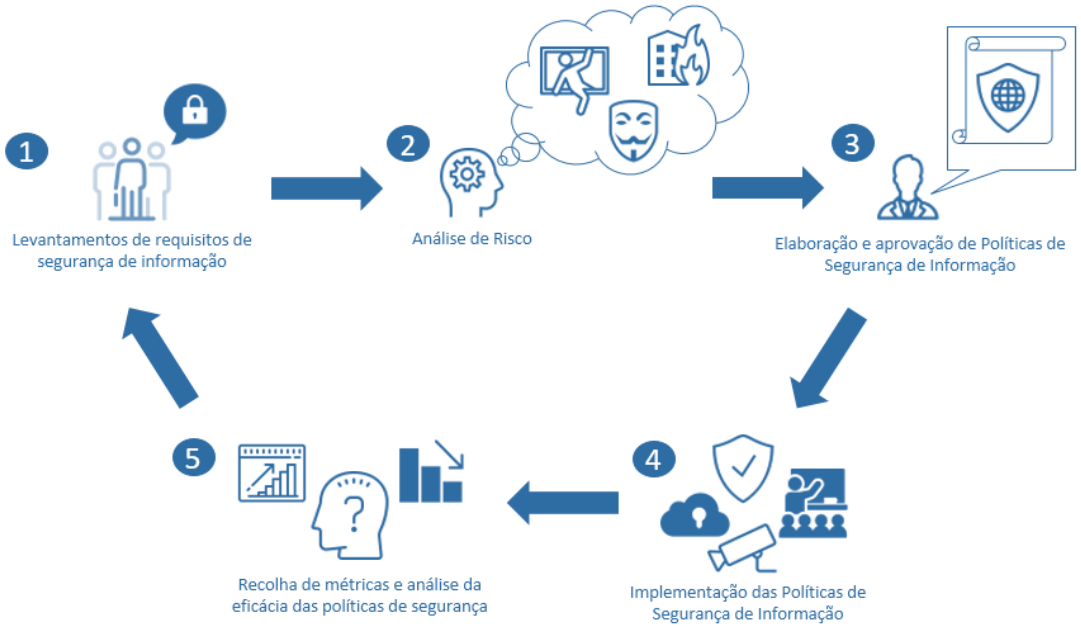


Figura 10- ciclo de vida das políticas de Segurança de Informação

2.5 Gestão de Risco

O QNRCS propõe uma implementação processual orientada à gestão do risco, que permita às organizações a tomada de decisão de forma priorizada e informada, no contexto da cibersegurança. Estas decisões devem, sempre, estar igualmente orientadas à garantia da confidencialidade, disponibilidade e integridade na prestação do bem ou serviço para uma determinada organização. Neste âmbito, entende-se risco como uma circunstância ou um evento identificável, com um potencial efeito adverso potencial na segurança das redes e dos sistemas de informação.

A gestão do risco, quando efetuada de forma sistematizada e numa lógica de melhoria, é uma prática que permite às organizações identificar, quantificar e estabelecer as prioridades face a critérios de aceitação do risco e objetivos relevantes para a organização.

A ISO/IEC 310001 disponibiliza um conjunto de princípios e de orientações genéricas sobre gestão do risco para as organizações. Por outro lado, a ISO/IEC 27005 especifica orientações e processos para gestão do risco de segurança dos sistemas de informação de uma organização, suportando-se, em particular, nos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI), implementado de acordo com a norma ISO/IEC 27001. A ISO/IEC 27005 não fornece uma metodologia específica para a gestão dos riscos de segurança da informação. Cabe às organizações definirem qual a sua abordagem para a gestão dos riscos. Em geral, a metodologia de gestão do risco ISO/IEC 27005, por ser direcionada a sistemas de informação, pode ser aplicável a todos os tipos de organização.

Figura 11 - Fases da Gestão de Risco, fonte: QNRCS

As medidas processuais e de caráter técnico a implementar poderão ser identificadas tendo por base o QNRCS e o enquadramento do risco, devendo ainda ter por objetivo a redução do nível do risco, ao ponto em que este possa ser considerado aceitável pela organização.

Capítulo 3 – Trabalho Empírico

Como pudemos ver no capítulo anterior, o QNRCS fornece orientações para a implementação de medidas de cibersegurança. No entanto, a falta de especificidade relativamente à aferição do risco, à relação entre a gestão de risco e a implementação das medidas do QNRCS ou falta de critérios que indiquem o que constituiria uma forma de "conformidade" com QNRCS, assumem-se como lacunas que a presente dissertação visa colmatar. Neste capítulo, definir-se-ão os pressupostos sobre os quais a tese se baseará, quer como forma de preenchimento das lacunas acima referidas, quer acerca dos elementos externos ao QNRCS (ex: empresa alvejada) usados para atestar a sua validade.

3.1 Empresa visada

QNRCS pretende ser aplicável, essencialmente, a organizações que assentem a sua atividade em tecnologia, quer seja numa perspetiva de cibersegurança para Tecnologias de Informação, de controlos de sistemas industriais, sistemas de interface homem-máquina, dispositivos IoT ou, de uma forma mais genérica, todos os dispositivos conectados de alguma forma a redes e sistemas de informação. A segurança de informação e a cibersegurança em particular são fatores chave para o sucesso e sobrevivência da organização.

A título de teste à implementação do QNRCS, esta tese recorre a uma PME real, cuja atividade se baseia em tecnologia e cujos serviços prestados se enquadram nas categorias de serviços digitais, descritas na lei 46/2018. De acordo com a tabela 2, esta organização encaixa-se na categoria de Micro Empresa, sendo constituída por um universo não superior a 10 pessoas.

A atividade desta organização exige uma forte cooperação com os seus fornecedores de serviços de TI ligados à operação, bem como com os seus clientes. A sua posição na cadeia de valor, missão e valores estão bem definidos, pois a indústria e o mercado em que opera, assim a obrigam. A sua motivação reside na sua vontade de se manter competitiva, melhorando a qualidade do seu serviço em simultâneo com a segurança.

Toda a implementação do QNRCS nesta tese – presente nos capítulos 3 e 4 – incidirá sobre esta organização, cujas dificuldades e desafios de implementação serão percecionadas como lições a aplicar a outras organizações de semelhante dimensão.

3.2 Quantificação das classificações dos objetivos dos QNRCS

A avaliação terá como base as classificações descritas no Quadro de Avaliação [2], já referidas no ponto 2.3. Contudo, as classificações do Quadro de Avaliação (Básico, Intermédio e Avançado) não contemplam casos em que a organização não tem qualquer medida que cumpra um determinado objetivo, nem casos para os quais a medida não se aplique. Assim, por cada subcategoria, aplicar-se-á um dos seguintes graus de maturidade:

- **Básico**[9] – aplica-se o nível Básico quando a descrição do objetivo e respetivas evidências se verificarem.
- **Intermédio** – aplica-se o Nível Intermédio quando as descrições do objetivo e respetivas evidências se verificam para os níveis Básico e Intermédio.
- **Avançado** – aplica-se o Nível Avançado quando as descrições do objetivo e respetivas evidências se verificam para os níveis Básico, Intermédio e Avançado.
- **<Em branco>** - aplica-se a ausência de qualquer classificação se nenhum dos critérios anteriores for correspondido.
- **N/A** – aplica-se a casos em que o objetivo em causa não se aplica.

Adicionalmente, será adotado um sistema de pontuação que se moldará consoante a classificação atribuída a cada objetivo. Assim, assumir-se-ão os seguintes valores:

- <Em branco> - 0 pontos.
- Básico – 1 ponto.
- Intermédio – 2 pontos.
- Avançado – 3 pontos.
- N/A – 3 pontos.

Note-se que a classificação de N/A ("não aplicável") corresponde à pontuação máxima, porque tal deve-se a que a avaliação concluiu que a **organização não possui superfície de ataque que justifique o cumprimento do objetivo,** e não tendo superfície de ataque, considera-se então que o nível de exposição é mínimo e, por conseguinte, equivalente ao cenário de classificação avançada.

É relevante referir que muitas empresas possuem vários serviços e diversas redes. Assim, a aplicação de um objetivo deve incidir apenas sobre o âmbito definido para aplicação do QNRCS, ou seja, a título de exemplo, se para o cumprimento de um objetivo, uma organização com 3 redes distintas (todas críticas para o negócio), e as 3 necessitarem de possuir um sistema de correlação de eventos (estão dentro do âmbito), e apenas duas das redes da organização o possuírem e a outra não, então o relatório deverá concluir que a organização não cumpre com o objetivo.

3.3 Conformidade com o QNRCS

O QNRCS define uma *framework* de resposta a incidentes e o quadro de avaliação do QNRCS define os graus de conformidade com cada objetivo. Porém, à data da produção deste documento, nenhum dos documentos define critérios para com a total conformidade da *framework*. A conformidade com uma *framework* é essencial para a organização não perder o

[9] Correspondente ao grau Inicial, esta tese optou por atribuir a designação de Básico a este nível, porque a designação Inicial pode indiciar o leitor que este grau de maturidade assume um cariz provisório, quando pode ser do interesse da organização manter o grau de maturidade mais baixo a uma determinada subcategoria.

foco da sua implementação, assegurando a existência de um objetivo de implementação para além da segurança de informação na organização. A definição desta conformidade deverá considerar:

1. Os objetivos da organização;
2. Os objetivos do QNRCS, nomeadamente a capacidade de Identificar, Proteger, Detetar, Responder e Recuperar.

Mas como se pode mensurar a conformidade do QNRCS à luz dos objetivos da organização? A resposta a esta pergunta é: através da matriz de risco. Assim, esta tese propõe-se relacionar a matriz de risco (através da análise ao hipotético total incumprimento de determinada subcategoria, como explicado na secção 3.4) com os 5 objetivos do QNRCS.

Neste sentido, a presente tese considera que a organização está em conformidade com o QNRCS se a organização:

1. possuir um processo de gestão de risco de cibersegurança;
2. cumprir com todos os objetivos aplicáveis ao seu âmbito, nomeadamente:
    a. Possuir 0 não-conformidades altas por objetivo;
    b. Garantir o cumprimentos dos 5 objetivos e 23 categorias;
    c. Possuir no máximo 20% de não-conformidades médias por objetivo (ex: 1 não-conformidade média em 5 possíveis no objetivo 'Recuperar').
    d. possuir no máximo até 25% não-conformidades baixas por objetivo.

Relativamente às não-conformidades, passa-se a considerar o seguinte:

- **não-conformidade alta**: incumprimento total de um processo (ex: gestão de risco) ou de subcategoria aplicável (não cumprimento do objetivo ID.GR1 quando o mesmo é aplicável) ou lacuna de 2 graus de maturidade ou superior, se o risco de incumprimento desse objetivo for Alto ou Crítico e o tratamento for a Mitigar ou Evitar.
- **não-conformidade média**: incumprimento parcial de uma subcategoria cuja lacuna corresponda a um grau de maturidade e cujo risco de incumprimento desse objetivo seja Alto ou Crítico e o tratamento for a Mitigar ou Evitar.
- **não-conformidade baixa**: qualquer incumprimento de um objetivo que não se enquadre no nas definições de não-conformidade média e alta.

Ao contrário da ISO/IEC 27001, o QNRCS não obriga à existência de um SoA[10], a qual define que controlos são aplicáveis à luz da gestão de risco – dentro do âmbito definido. No entanto, tal como na ISO 27001, esta tese propõe-se a identificar quais os objetivos aplicáveis, pelo que o mesmo método tem de ser aplicado. Assim, a matriz de gestão de risco servirá também como documento equivalente ao Estado da Aplicabilidade da ISO 27001, conforme veremos a seguir.

[10] State of Aplicability (Estado da aplicabilidade), ISO/IEC 27001 (2013), cláusula 6.1.3

Deste modo, a fim de definir os objetivos aplicáveis, ter-se-á de proceder a uma análise de risco.

3.4 Metodologia de gestão de risco

Conforme referenciado no QNRCS [1], a metodologia de análise do risco pode ser consubstanciada por uma abordagem analítica de caráter qualitativo, quantitativo ou por uma combinação de ambas. Na prática, a análise qualitativa é mais utilizada, numa primeira abordagem, para a obtenção de indicadores gerais do nível do risco e para identificar os riscos mais relevantes.

Assim, de forma a que o processo de análise de risco seja auditável, é recomendável que o mesmo seja documentado. Esta documentação pode ser obtida através de vários formatos - ficheiros (ex: Excel), aplicações web ou outros meios. Por isso, este documento deverá enumerar os riscos, avaliar os mesmos à luz de identificação de vulnerabilidades e ameaças, probabilidade e o seu impacto na Confidencialidade, Integridade e Disponibilidade, mas não apenas. Nos critérios de aferição do impacto do risco, devem ser igualmente observadas as seguintes dimensões (em linha com as recomendações do QNRCS [1]):

- **Reputação** – A ocorrência de determinado risco pode colocar em causa a reputação da organização (por exemplo: perda de confiança das partes interessadas);
- **Legal ou Regulatório** – A ocorrência de determinado risco poderá colocar em causa responsabilidades legais e/ou regulatórias da organização (por exemplo: responsabilidades regulatórias sectoriais);
- **Serviço a clientes** – A ocorrência de determinado risco poderá colocar em causa o serviço prestado aos clientes da organização (por exemplo: incumprimento de um nível de serviço);
- **Financeiro** – A ocorrência de determinado evento pode levar a que a organização possa incorrer em custos financeiros não previstos (por exemplo: coimas, recursos adicionais).

Assim, a análise do risco define-se através da avaliação do impacto de um determinado evento (risco) e da avaliação da probabilidade desse evento ocorrer. Neste sentido, podemos quantificar o risco como sendo **Risco = Impacto x Probabilidade.**

Tendo em mente as dimensões das PMEs e o tempo usualmente disponível para se dedicar à avaliação do risco, a presente tese apresenta uma solução de quantificação do risco baseada em 3 graus de Impacto e 3 graus[11] de Probabilidade para a PME visada neste trabalho:

[11] O QNRCS refere um exemplo em que a matriz de classificação de risco é composta por 16 hipóteses (4x4). Contudo, o exemplo é meramente ilustrativo, havendo liberdade do lado da organização definir a sua própria matriz de classificação de risco. Uma matriz de classificação de risco composta de 9 hipóteses (3x3), adequa-se à dimensão da organização visada nesta tese.

		Probabilidade		
		1	2	3
Impacto	1	1	2	3
	2	2	4	6
	3	3	6	9

Tabela 5 - Matriz de classificação de Risco

Risco	Designação
1; 2	Baixo
3;4	Médio
6	Alto
9	Crítico

Tabela 6 - Quantificação do Risco

Nesta fase, caberá à organização definir o seu grau de aceitação ao risco, definindo a estratégia de tratamento do risco. Conforme alinhado com as melhores práticas (e em linha com a recomendação do QNRCS [1]), foram definidos 4 tipos de tratamento de risco:

- **Evitar o risco:** colocar a probabilidade ou impacto tendencialmente próximo de zero, tornando mais difícil a sua ocorrência e/ou eliminar totalmente o seu impacto;
- **Aceitar o risco**: decisão de aceitação do risco. A assunção de responsabilidade por essa decisão deve ser formalmente registada pela organização;
- **Mitigar o risco**: reduzir a probabilidade e/ou impacto de um evento adverso para limites aceitáveis, através da implementação de controlos ou contramedidas;
- **Transferir o risco**: transferir, total ou parcialmente, para terceiras partes, o impacto em relação a uma ameaça (por exemplo: efetuar a contratualização de um seguro).

3.4.1 Quantificação do Impacto

Conforme referido acima, o impacto do risco deve ter como base as vulnerabilidades, as ameaças identificadas e as respetivas consequências do risco nos ativos e processos referentes à atividade da organização. Assim, e tendo como base o "valor" da informação que se pretende proteger à luz da Confidencialidade, Integridade e Disponibilidade, define-se o valor da informação da seguinte forma:

	Baixa - 1	Média - 2	Elevada - 3
Confidencialidade	O acesso não autorizado à informação tem um efeito adverso **limitado** nas operações, bens ou na comunidade	O acesso não autorizado à informação tem um efeito adverso **significativo** nas operações, bens ou na comunidade	O acesso não autorizado à informação tem um efeito adverso **catastrófico** nas operações, bens ou na comunidade
Integridade	Uma alteração não autorizada à	Uma alteração não autorizada à	Uma alteração não autorizada à

	informação ou destruição da mesma tem um efeito **limitado** nas operações, bens ou na comunidade	informação ou destruição da mesma tem um efeito **significativo** nas operações, bens ou na comunidade	informação ou destruição da mesma tem um efeito **catastrófico** nas operações, bens ou na comunidade
Disponibilidade	O não acesso ou impossibilidade de utilização da informação ou sistema de informação tem um efeito **limitado** nas operações, bens ou na comunidade	O não acesso ou impossibilidade de utilização da informação ou sistema de informação tem um efeito **significativo** nas operações, bens ou na comunidade	O não acesso ou impossibilidade de utilização da informação ou sistema de informação tem um efeito **catastrófico** nas operações, bens ou na comunidade

Tabela 7 - Impacto em função do CIA (Confidencialidade, Integridade e Disponibilidade

Com base nas melhores práticas e à dimensão da organização, o impacto será quantificado em 3 níveis:

Impacto		
Nível	Valor	Condição
Baixo	1	Se a combinação Confidencialidade, Integridade e Disponibilidade for do tipo – **Baixa |Baixa ou Baixa |Baixa |Baixa**
Médio	2	Se a combinação Confidencialidade, Integridade e Disponibilidade for do tipo – **Média |Baixo |Elevada** ou **Média |Média** ou **Média |Média| Média**
Elevado	3	Se a combinação Confidencialidade, Integridade e Disponibilidade for do tipo – **Elevada |Elevada |Elevada** ou **Elevada |Elevada**

Tabela 8 - Quantificação do Impacto

3.4.2 Quantificação da Probabilidade

Uma vez identificados os cenários de incidentes, incluindo identificação de ameaças, ativos afetados, vulnerabilidades exploradas e o impacto para os ativos e para os processos referentes à atividade da organização, deve ser tido em linha de conta a frequência da ocorrência das ameaças e a facilidade com que as vulnerabilidades poderão ser exploradas, considerando:

a) Experiência e estatísticas aplicáveis para a probabilidade de ameaça;

b) Para fontes de ameaças humanas: a **motivação** e as capacidades que mudam com o tempo e os recursos disponíveis para um possível atacante, bem como a perceção de atratividade e da vulnerabilidade dos ativos;
c) Para fontes de ameaças acidentais: fatores geográficos, como por exemplo proximidade com indústrias químicas ou petrolíferas, a possibilidade de condições climáticas;
d) Vulnerabilidades, individualmente ou em conjunto.

Assim, definem-se 3 níveis de tipificação para a Probabilidade, baseados nas melhores práticas e adaptados às dimensões da organização:

Probabilidade		
Nível	Valor	Probabilidade
Improvável	1	Probabilidade de o evento ocorrer inferior a uma vez em cada 3 anos.
Provável	2	Probabilidade de o evento ocorrer entre uma vez em cada 3 anos e uma vez por ano.
Muito Provável	3	Probabilidade de o evento ocorrer superior a uma vez por ano

Tabela 9 - Quantificação da Probabilidade

Nota: a probabilidade pode estar (mas não necessariamente) diretamente relacionada com a exposição da organização. Mediatismo e projeção nos meios de comunicação social, entre outros canais, aumenta a probabilidade de a organização ser alvo de ataque.

3.4.3 Estratégia de tratamento de risco

Face às estratégias definidas acima e às categorizações do risco, assume-se a seguinte estratégia de avaliação de risco para a PME visada:

Risco Crítico (9): Este nível de risco é **inadmissível** e não é **transferível**, pelo que só é aceitável que seja **evitado** ou **mitigado**.

Risco Alto (6): Este nível de risco acarreta que ou a probabilidade é elevado ou o impacto é elevado, pelo que a sua **aceitação não é equacionável**. Porém, se se tratar de uma probabilidade alta e um impacto médio, o risco pode ser **transferível**, **mitigado** ou **evitado**; mas se o impacto for elevado e a probabilidade média, então o risco apenas pode ser **mitigado** ou **evitado**.

Risco médio (3-4): Este nível de risco porta a possibilidade de o impacto ou a probabilidade serem elevados (apesar de a sua probabilidade ou impacto respetivamente serem baixos).

Para estes casos, fará sentido equacionar a mitigação ou a evitação se o impacto for elevado e a transferência e a evitação se a probabilidade for elevada. Para o caso de o valor do risco ser igual a 4, então sugere-se a transferência e a evitação.

Risco baixo (1-2): Este nível de risco é aceitável, pelo que a sua aceitação ou transferência são aceitáveis.

3.4.4 Análise do Risco

Tal como indicado anteriormente, a matriz de risco servirá como ferramenta para atestar à análise do risco de cibersegurança, bem como terá a função equivalente ao Estado da Aplicabilidade da ISO/IEC 27001 na medida que avaliará a necessidade de aplicar os "controlos" ou grau de maturidade dos níveis dos objetivos do QNRCS. Com efeito, a análise de risco adotada para esta tese **propõe-se a avaliar qual o risco da total ausência deste objetivo na organização (ou seja, para cada caso objetivo do QNRCS avaliar o risco de o mesmo não ser cumprido)**, e posteriormente considerar outros riscos que, não sendo contemplados na avaliação da ausência dos controlos, possam ser mitigados através dos controlos existentes ou através da adição de controlos adicionais.

Para efeito de controlo de risco, define-se para a PME visada, a seguinte matriz de risco, com as colunas:

ID do Risco	Descrição do risco	Vulnerabilidade	Ameaça	Ativo	Confidencialidade	Integridade	Disponibilidade	Impacto	Probabilidade	Nível do Risco	Tratamento de Risco	Maturidade Alvo	Responsável do Risco
1	…	…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…	…	…

Figura 12 - Colunas da Matriz de Risco

A título de exemplo, observe-se o preenchimento de uma linha da matriz de risco, com a respetiva explicação da coluna:

- **ID do Risco** – número inteiro único que define uma linha. Ex: 1.
- **Descrição do Risco**[12] - Uma circunstância ou um evento razoavelmente identificável, com um efeito adverso potencial na segurança das redes e dos sistemas de informação. Ex: *Perda de equipamento*.
- **Vulnerabilidade** - Fraqueza de um ativo ou de um controlo que pode ser explorada por uma ameaça. Ex: *Dispositivos físicos, redes e sistemas de informação existentes na organização (e incluídos no âmbito) não estarem inventariados*.

[12] Definição do QNRCS, página. 20 [1]

- **Ameaça** - Potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização (que surge como exploração da vulnerabilidade). Ex: *Furto não detetado de equipamento*.
- **Ativo** – Algo com valor para uma organização. Ex: *equipamento informáticos com informação contida: discos, pen drives, workstations, componentes de infraestrutura de TI*.
- **Confidencialidade** – Potencial impacto na confidencialidade da informação. A preencher com os valores definidos na secção do impacto (Baixo (1), Médio (2), Elevado (3)). Ex: 3
- **Integridade** - Potencial impacto na integridade da informação. A preencher com os valores definidos na secção do impacto (Baixo (1), Médio (2), Elevado (3)). Ex: 2
- **Disponibilidade** - Potencial impacto na disponibilidade da informação. A preencher com os valores definidos na secção do impacto (Baixo (1), Médio (2), Elevado (3)). Ex: 3
- **Impacto** – Valor do impacto deduzido de acordo com os critérios definidos na secção 3.3.1 Quantificação de impacto (Baixo (1), Médio (2), Elevado (3)). Ex: 3
- **Probabilidade** – Valor da probabilidade de acordo com os critérios definidos em 3.3.2 Quantificação da probabilidade (Improvável (1), Provável (2), Muito Provável (3)). Ex: 2
- **Nível de Risco** – Valor quantificado do risco de acordo com as definições da tabela 7 e tabela 8. Ex: 6 (probabilidade (2) x impacto (3))
- **Tratamento de Risco** – Tratamento do risco à luz dos critérios definidos na secção 3.3.3 Estratégia de tratamento de risco. Ex: Mitigar risco
- **Ações/ Controlo** – Descrição dos controlos a aplicar para mitigar o risco identificado. Pode ser qualquer ação que o responsável do risco entenda adequada (texto livre). Porém, a título de aferição da aplicabilidade dos objetivos do QNRCS, as soluções protagonizadas pelo do QNRCS têm de ser contempladas. Assim, podemos atribuir a designação13 do objetivo que vise a mitigação do risco correspondente. Ex: ID.GA-1
- **Grau de Maturidade** – Se a ação ou controlo descrita na coluna anterior designar um objetivo do QNRCS, então este campo deve identificar o grau de maturidade do objetivo do QNRCS de acordo com os critérios do Quadro de Avaliação de Capacidades Mínimas em Cibersegurança [2]. Exemplo: Intermédio.
- **Responsável do Risco** – Designa a pessoa ou cargo responsável pelo tratamento do risco. Ex: responsável de TI.

Para além do exemplo do risco referido acima, importa também considerar riscos cujas vulnerabilidades e ameaças se encontram definidos na taxonomia da rede CSIRT [3].

[13] De acordo com as designações e implementações descritas no Quadro de Avaliação de Capacidades Mínimas em Cibersegurança [2].

Por fim, o risco remanescente após tratamento deve ser considerado, pelo que cada risco remanescente é visto como um risco novo, ou seja, uma nova entrada (linha) na matriz de risco.

3.5 Prioridade e âmbito (Passo 1)

O QNRCS difere da norma ISO/IEC 27001 no sentido em que o primeiro se foca sobretudo na cibersegurança e o segundo na segurança de informação (que engloba entre outras matérias, a cibersegurança). Contudo, ambas partilham dos mesmos princípios base: Confidencialidade, Integridade e Disponibilidade.

O objetivo da implementação da cibersegurança em qualquer organização é a proteção da sua operação. Neste sentido, o âmbito da cibersegurança deve incidir sobre os processos de suporte ao negócio/operação (ex: suporte informático, atividade administrativa, recursos humanos que dependam do uso da infraestrutura de TI) e em alguns casos, na própria operação quando a mesma assenta em tecnologias de TI.

É importante salientar que enquanto o método de definição de âmbito ISO/IEC 27001 se foca na informação que se pretende proteger e de deduzindo-se de seguida os processos da organização que processam esta informação e consequentemente os ativos de informação presentes nestes processos. A definição do âmbito do QNRCS foca-se na informação que se pretende proteger e daí inferindo diretamente os ativos que processam esta informação. A escolha da informação que se pretende proteger deve ser avaliada à luz do risco e dos impactos financeiros, reputacionais e legais.

Também não é demais lembrar que as organizações mais pequenas usualmente aproveitam os mesmos recursos, quer humanos, quer de TI, tanto na operação como nos processos de suporte (como resultado do reduzido número de recursos). Como tal, será normal incluir todos estes processos sobre o mesmo âmbito.

Assim, na **PME visada nesta tese de mestrado**, a **sua operação** assenta na sua infraestrutura de TI, razão pela qual será imperativo inclui-la no âmbito. Contudo, como os **processos de suporte** também dependem substancialmente da mesma infraestrutura de TI, então os ativos de informação (ex: recursos humanos) incluídos nas atividades de suporte também serão abrangidos no âmbito.

Ainda dentro desta fase, cabe a organização definir as suas opções estratégicas quanto à implementação de medidas de cibersegurança. Estas estratégias incluem:

- Periodicidade da revisão do QNRCS: Não havendo (à data) uma obrigatoriedade de implementação do QNRCS, nem critérios de certificação, não existe nenhum período definido estabelecido para a revisão da adequação do QNRCS. Assim, será importante definir um processo de revisão da implementação do QNRCS.

- Tempo de implementação das medidas de cibersegurança: uma vez identificadas as lacunas de cibersegurança, será necessário definir um plano de atividade de implementação. Este tempo deve ser adequado à dimensão e capacidade de recursos da organização.

Note-se que para aferir acerca destes tempos, é importante ter em consideração os tempos de longevidade e de expansão da atividade das organizações. Se uma organização expandir a sua atividade, o âmbito da implementação do programa de cibersegurança poderá ter que ser revisto, e consequentemente a implementação do QNRCS. Simultaneamente é importante ter em conta que o tempo reservado para a implementação do plano de ação previsto no Passo 7 (secção 2.4), deve ser compatível com o tempo de revisão do programa de cibersegurança.

Com base no que foi dito acima, para a PME visada, adota-se a seguinte estratégia:

1. Revisão total do âmbito do programa de cibersegurança com periodicidade **trianual**: no caso da organização visada, não é expectável uma mudança na natureza da sua atividade, pelo que atendendo à análise efetuada ao risco, a revisão do âmbito do programa da cibersegurança é perfeitamente adequada à sua atividade.
2. Revisão total da matriz de risco com periodicidade anual: a matriz de risco deve ser alvo de constante atualização. Porém, a implementação anual sua revisão total, garante que o risco de cibersegurança é revisto pelo menos uma vez por ano. Desta reavaliação da matriz de risco, poderão deduzir-se novas ações ou uma nova priorização de tratamentos de risco.
3. Planos de ação anuais: O plano de ação deve ser articulado com a revisão da matriz de risco. Assim, o plano de ação abordará primeiramente as implementações mais críticas e depois as menos críticas. Neste caso em particular, opta-se por adereçar primeiro todas as não-conformidades graves, e depois as não-conformidades menos graves. Todas as não-conformidades altas devem ser resolvidas dentro do intervalo de tempo destinado ao plano de ação (coincidente com o período de reavaliação de risco), e todas as não-conformidades baixas devem ser resolvidas dentro do período coincidente com a revisão do âmbito.

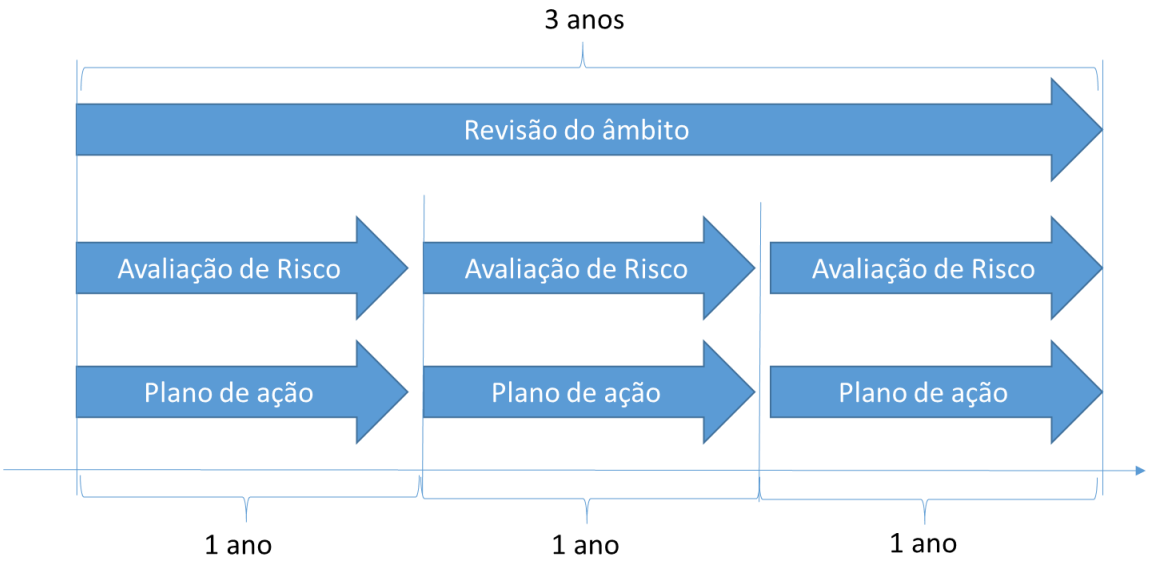


Figura 13 - Estratégia do programa de cibersegurança

3.6 Linhas orientadoras – ativos e implementações (Passo 2)

Após determinação do âmbito, segue-se a definição dos ativos de informação. Neste sentido consideram-se ativos de informação todos:

- Sistemas de informação: redes e sistemas informáticos que suportam a operação e os processos de suporte. Especificamente, inclui a infraestrutura de TI da sede de operação (*firewall*, *switches*, *workstations*, …) e infraestrutura de *datacenter* (*firewall*, *switches*, *servidores, load balancers* ...);
- Recursos humanos: colaboradores que manuseiam os sistemas de informação e que têm acesso à informação que se pretende proteger.

Em suma, estes ativos englobam todos os colaboradores, a quase totalidade dos sistemas de informação em três geografias distintas. A cadeia de fornecedores e clientes (em contacto com a informação que se pretende proteger e com os sistemas de informação incluídos no âmbito) também é considerada no âmbito do programa da cibersegurança.

O plano das atividades de implementação deve priorizar a correção das não-conformidades dentro de cada objetivo, de forma a cumprir os requisitos de conformidade definidos na secção 3.3. A correção das não-conformidades deve priorizar a ordem dos objetivos do QNRCS, ou seja, começar a correção das não-conformidades do objetivo 'Identificar', e depois seguir para a correção das não-conformidades do objetivo seguinte e assim adiante[14].

[14] Os objetivos do QNRCS são interdependentes, pelo que não se podem proteger ativos sem antes os identificar, e não se podem detetar eventos de segurança em ativos se os mesmos não estiverem protegidos, e assim adiante.

Capítulo 4 – Resultados

Este capítulo descreve os processos que compõem o *Gap Analysis*, nomeadamente:

1. Processo de criação de Perfil Atual (Passo 3)
2. Aferição do Risco (Passo 4)
3. Criação do Perfil Alvo (Passo 5)

O processo de *Gap Analysis*, que habitualmente se fará em cada intervalo de Avaliação de Risco (conforme definido na secção 3.4) irá determinar as lacunas de segurança.

4.1 Processo de criação de Perfil Atual (Passo 3)

O processo de criação de Perfil Alvo é elaborado segundo as referências do Quadro de Avaliação das Capacidades Mínimas de Cibersegurança [2]. Esta análise foi efetuada consultando diretamente o documento do CNCS[15], mas alternativamente pode ser efetuada na ferramenta de *cibercheckup*[16] disponível na página web do CNCS.

O processo de criação de perfil atual do objetivo de '*Identificar*':

OBJECTIVO	CATEGORIA	Abreviatura	GRAU DE MATURIDADE	Pontuação
IDENTIFICAR	ID.GA - Gestão de ativos	ID.GA-1	Básico	1
		ID.GA-2	Básico	1
		ID.GA-3	Básico	1
		ID.GA-4	Intermédio	2
		ID.GA-5	----------	0
	ID.AO - Ambiente da Organização	ID.AO-1	Básico	1
		ID.AO-2	Básico	1
		ID.AO-3	Básico	1
		ID.AO-4	Básico	1
		ID.AO-5	Intermédio	2
	ID.GV - Governação	ID.GV-1	----------	0
		ID.GV-2	Básico	1
	ID.AR - Avaliação de risco	ID.AR-1	Básico	1
		ID.AR-2	----------	0
		ID.AR-3	----------	0
		ID.AR-4	----------	0

[15] Quadro de Avaliação de Capacidades Mínimas em Cibersegurança [2]

[16] https://cibercheckup.cncs.gov.pt/

		ID.AR-5	Básico	1
	ID.GR - Estratégia de Gestão de Risco	ID.GR-1	Básico	1
		ID.GR-2	Básico	1
		ID.GR-3	Básico	1
	ID.GL – Gestão do Risco da Cadeia Logística	ID.GL-1	Básico	1
		ID.GL-2	Básico	1
		ID.GL-3	----------	0
		ID.GL-4	Básico	1
		ID.GL-5	Avançado	3

Tabela 10 - Perfil atual do objetivo Identificar

Como a maior parte das organizações pequenas e médias dimensões, a PME analisada dispõe de processos de gestão de risco contundentes e pouco oleados. Apesar disso, é evidente a perceção existente do risco de segurança associado à sua operação e à sua posição na cadeia de valor, bem como a necessidade de inventariar os seus ativos.

A média pontual arredondada da organização, no objetivo de '*Identificar'* é de **1** (Básico).

O processo de criação de perfil atual do objetivo de '*Proteger'*:

OBJECTIVO	CATEGORIA	Abreviatura	GRAU DE MATURIDADE	Pontuação
PROTEGER	PR.GA – Gestão de Identidades, Autenticação e Controlo de Acessos	PR.GA-1	Intermédio	2
		PR.GA-2	Básico	1
		PR.GA-3	Intermédio	2
		PR.GA-4	Intermédio	2
		PR.GA-5	Intermédio	2
		PR.GA-6	Básico	1
		PR.GA-7	Básico	1
	PR.FC – Formação e Sensibilização	PR.FC-1	Básico	1
		PR.FC-2	Básico	1
		PR.FC-3	Básico	1
		PR.FC-4	Básico	1
	PR.SD – Segurança de Dados	PR.SD-1	----------	0
		PR.SD-2	Básico	1
		PR.SD-3	Básico	1
		PR.SD-4	Intermédio	2
		PR.SD-5	----------	0
		PR.SD-6	Intermédio	2
		PR.SD-7	----------	0
		PR.SD-8	Intermédio	2
	PR.PI – Procedimentos e	PR.PI-1	Básico	1

	Processos de Proteção da Informação	PR.PI-2	N/A	3
		PR.PI-3	Intermédio	2
		PR.PI-4	Básico	1
		PR.PI-5	Intermédio	2
		PR.PI-6	Básico	1
		PR.PI-7	Básico	1
		PR.PI-8	Básico	1
		PR.PI-9	Básico	1
		PR.PI-10	Básico	1
		PR.PI-11	Básico	1
		PR.PI-12	Básico	1
	PR.MA – Manutenção	PR.MA-1	Intermédio	2
		PR.MA-2	Intermédio	2
	PR.TP – Tecnologia de Proteção	PR.TP-1	Básico	1
		PR.TP-2	----------	0
		PR.TP-3	Intermédio	2
		PR.TP-4	Intermédio	2
		PR.TP-5	Avançado	3

Tabela 11 - Perfil atual do objetivo Proteger

A organização tem bem clara a necessidade de proteger a sua infraestrutura contra os problemas de cibersegurança mais comuns. Porém, devido a desconhecimento ou à falta de perceção de risco, não possui um processo de gestão de vulnerabilidades robusto, sendo este tipo de procedimento reativo.

A média pontual arredondada da organização, no objetivo de '*Proteger'* é de **1** (Básico).

O processo de criação de perfil atual do objetivo de '*Detetar'*:

OBJECTIVO	CATEGORIA	Abreviatura	GRAU DE MATURIDADE	Pontuação
DETETAR	DE.AE – Anomalias e Eventos	DE.AE-1	Intermédio	2
		DE.AE-2	Básico	1
		DE.AE-3	Básico	1
		DE.AE-4	----------	0
		DE.AE-5	----------	0
	DE.MC – Monitorização Contínua de Segurança	DE.MC-1	Intermédio	2
		DE.MC-2	Intermédio	2
		DE.MC-3	----------	0
		DE.MC-4	Básico	1

		DE.MC-5	N/A	3
		DE.MC-6	N/A	3
		DE.MC-7	----------	0
		DE.MC-8	----------	0
	DE.PD – Processos de Deteção	DE.PD-1	Básico	1
		DE.PD-2	Básico	1
		DE.PD-3	Básico	1
		DE.PD-4	Básico	1
		DE.PD-5	Básico	1

Tabela 12 - Perfil atual do objetivo Detetar

O processo de Deteção da organização beneficia de apoio de fornecedores externos no processo de deteção dos incidentes nos seus sistemas mais críticos. Contudo, os restantes sistemas e processos (não críticos, mas de suporte) possuem mecanismos de deteção contundentes.

A média pontual arredondada da organização, no objetivo de '*Detetar'* é de **1** (Básico).

O processo de criação de perfil atual do objetivo de '*Responder'*:

OBJECTIVO	CATEGORIA	Abreviatura	GRAU DE MATURIDADE	Pontuação
RESPONDER	RS.PR – Planeamento da Resposta	RS.PR-1	Básico	1
	RS.CO – Comunicações	RS.CO-1	Básico	1
		RS.CO-2	Básico	1
		RS.CO-3	Intermédio	2
		RS.CO-4	Intermédio	2
		RS.CO-5	Intermédio	2
	RS.AN – Análise	RS.AN-1	----------	0
		RS.AN-2	Básico	1
		RS.AN-3	----------	0
		RS.AN-4	----------	0
		RS.AN-5	Básico	1
	RS.MI – Mitigação	RS.MI-1	Básico	1
		RS.MI-2	Básico	1
		RS.MI-3	----------	0
	RS.ME – Melhorias	RS.ME-1	Avançado	3
		RS.ME-2	----------	0

Tabela 13 - Perfil atual do objetivo Responder

Os processos de resposta encontram-se razoavelmente oleados, substancialmente justificado pelos anos de operação e da aprimoração de processos de resposta (ainda que de forma não sistematizada).

A média pontual arredondada da organização, no objetivo de '*Responder'* é de **1** (Básico).

O processo de criação de perfil atual do objetivo de '*Recuperar'*:

OBJECTIVO	CATEGORIA	Abreviatura	GRAU DE MATURIDADE	Pontuação
RECUPERAR	RC.PR – Plano de Recuperação	RC.PR-1	Intermédio	2
	RC.ME – Melhorias	RC.ME-1	Intermédio	2
		RC.ME-2	Básico	1
	RC.CO – Comunicações	RC.CO-1	Básico	1
		RC.CO-2	Intermédio	2

Tabela 14 - Perfil atual do objetivo Recuperar

Tal como os processos de resposta, os processos de recuperação encontram-se relativamente oleados, fruto da melhoria contínua (não sistematizada) dos processos de recuperação. Além disso, existe uma maior preocupação com a Disponibilidade do que os outros pilares da segurança de informação (sem prejuízo dos destes).

A média pontual arredondada da organização, no objetivo de '*Recuperar'* é de **2** (Intermedio).

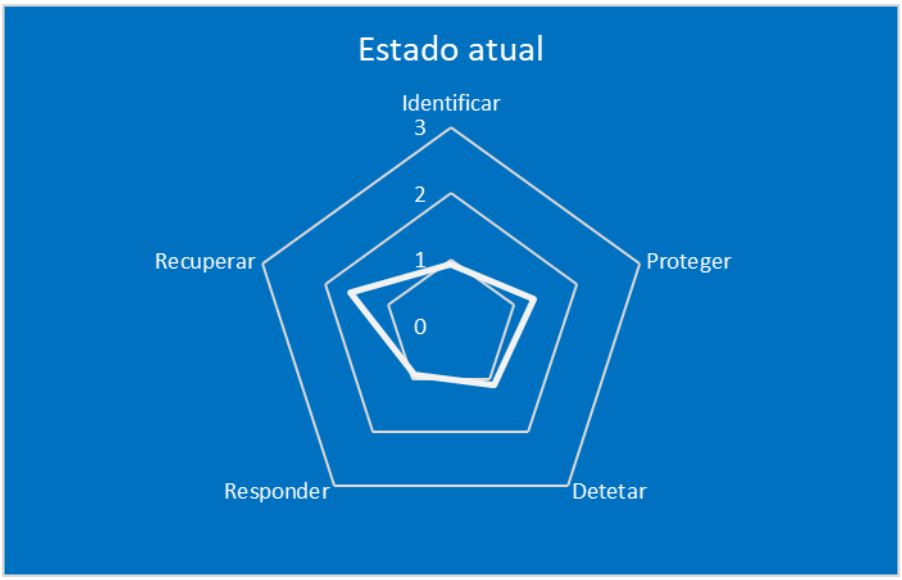


Figura 14 - Estado Atual (valores médios)

Em suma, muitos dos controlos já existentes são fruto da experiência da organização e de lições aprendidas ao longo de 20 anos de existência. No entanto, a maioria ou totalidade das lacunas devem-se à falta de recursos ou à falta da perceção de risco, dois fatores comuns em várias pequenas e médias empresas.

4.2 Aferição do Risco (Passos 4 e 5)

Conforme referido na secção 3.3.4 Análise de Risco, a avaliação de risco teve em conta os cenários de risco do que seria a total ausência dos controlos / objetivos do QNRCS, entre outros cenários. Esta análise específica tem por base a aferição da aplicabilidade das medidas do QNRCS[17].

Impacto	Probabilidade	Nível do Risco[18]	Tratamento do Risco	Ações / Subcategorias[19]	Maturidade Alvo
3	2	6	Mitigar o risco	ID.GA-1	Intermédio
2	1	2	Mitigar o risco	ID.GA-2	Básico
3	1	3	Mitigar o risco	ID.GA-3	Intermédio
1	3	3	Mitigar o risco	ID.GA-4	Intermédio
2	2	4	Mitigar o risco	ID.GA-5	Básico
2	1	2	Aceitar o risco	ID.AO-1	Básico
2	1	2	Aceitar o risco	ID.AO-2	Básico
1	1	1	Aceitar o risco	ID.AO-3	Básico
2	2	4	Mitigar o risco	ID.AO-4	Básico
3	2	6	Mitigar o risco	ID.AO-5	Avançado
2	2	4	Mitigar o risco	ID.GV-1	Intermédio
3	2	6	Mitigar o risco	ID.GV-2	Avançado
3	2	6	Mitigar o risco	ID.AR-1	Intermédio
2	1	2	Mitigar o risco	ID.AR-2	Intermédio
3	1	3	Mitigar o risco	ID.AR-3	Intermédio
3	1	3	Mitigar o risco	ID.AR-4	Intermédio
2	1	2	Mitigar o risco	ID.AR-5	Básico
2	2	4	Mitigar o risco	ID.GR-1	Intermédio
1	2	2	Mitigar o risco	ID.GR-2	Básico
2	1	2	Aceitar o risco	ID.GR-3	Básico
2	2	4	Mitigar o risco	ID.GL-1	Intermédio
2	1	2	Mitigar o risco	ID.GL-2	Básico
3	1	3	Mitigar o risco	ID.GL-3	Intermédio
2	1	2	Mitigar o risco	ID.GL-4	Básico

[17] Os riscos considerados; ativos; vulnerabilidades e ameaças identificadas para cada ausência de controlo encontram-se omitidos.

[18] Conforme descrito na tabela 5

[19] Subcategorias do QNRCS

3	2	6	Mitigar o risco	ID.GL-5	Avançado
2	3	6	Mitigar o risco	PR.GA-1	Intermédio
2	2	4	Mitigar o risco	PR.GA-2	Básico
3	3	9	Mitigar o risco	PR.GA-3	Avançado
3	1	3	Mitigar o risco	PR.GA-4	Avançado
2	2	4	Mitigar o risco	PR.GA-5	Intermédio
3	1	3	Mitigar o risco	PR.GA-6	Básico
3	1	3	Mitigar o risco	PR.GA-7	Básico
2	3	6	Evitar o risco	PR.FC-1	Intermédio
2	2	4	Mitigar o risco	PR.FC-2	Básico
2	2	4	Mitigar o risco	PR.FC-3	Básico
3	2	6	Mitigar o risco	PR.FC-4	Intermédio
2	2	4	Mitigar o risco	PR.SD-1	Básico
2	1	2	Mitigar o risco	PR.SD-2	Básico
2	1	2	Mitigar o risco	PR.SD-3	Básico
3	2	6	Mitigar o risco	PR.SD-4	Intermédio
2	1	2	Mitigar o risco	PR.SD-5	Básico
3	2	6	Mitigar o risco	PR.SD-6	Intermédio
2	1	2	Aceitar o risco	PR.SD-7	Básico
2	3	6	Mitigar o risco	PR.SD-8	Intermédio
2	1	2	Mitigar o risco	PR.PI-1	Básico
2	2	4	Evitar o risco	PR.PI-2	Básico
3	2	6	Mitigar o risco	PR.PI-3	Intermédio
3	2	6	Mitigar o risco	PR.PI-4	Avançado
3	2	6	Mitigar o risco	PR.PI-5	Intermédio
2	3	6	Mitigar o risco	PR.PI-6	Intermédio
2	3	6	Mitigar o risco	PR.PI-7	Intermédio
2	3	6	Mitigar o risco	PR.PI-8	Intermédio
3	2	6	Mitigar o risco	PR.PI-9	Intermédio
3	2	6	Mitigar o risco	PR.PI-10	Intermédio
1	1	1	Aceitar o risco	PR.PI-11	Básico
2	3	6	Mitigar o risco	PR.PI-12	Intermédio
3	2	6	Mitigar o risco	PR.MA-1	Intermédio
3	2	6	Mitigar o risco	PR.MA-2	Intermédio
2	2	4	Mitigar o risco	PR.TP-1	Básico
2	2	4	Mitigar o risco	PR.TP-2	Básico
3	3	9	Mitigar o risco	PR.TP-3	Avançado
3	2	6	Mitigar o risco	PR.TP-4	Intermédio
3	2	6	Mitigar o risco	PR.TP-5	Avançado

3	2	6	Mitigar o risco	DE.AE-1	Intermédio
3	2	6	Mitigar o risco	DE.AE-2	Intermédio
3	2	6	Mitigar o risco	DE.AE-3	Avançado
3	2	6	Mitigar o risco	DE.AE-4	Intermédio
3	1	3	Mitigar o risco	DE.AE-5	Básico
3	2	6	Mitigar o risco	DE.MC-1	Avançado
3	2	6	Mitigar o risco	DE.MC-2	Intermédio
2	2	4	Mitigar o risco	DE.MC-3	Básico
3	2	6	Mitigar o risco	DE.MC-4	Intermédio
2	2	4	Evitar o risco	DE.MC-5	Básico
3	1	3	Evitar o risco	DE.MC-6	Básico
3	2	6	Mitigar o risco	DE.MC-7	Intermédio
3	2	6	Mitigar o risco	DE.MC-8	Intermédio
3	1	3	Mitigar o risco	DE.PD-1	Básico
3	1	3	Mitigar o risco	DE.PD-2	Básico
2	2	4	Mitigar o risco	DE.PD-3	Intermédio
3	2	6	Mitigar o risco	DE.PD-4	Intermédio
2	2	4	Mitigar o risco	DE.PD-5	Intermédio
3	2	6	Mitigar o risco	RS.PR-1	Intermédio
3	2	6	Mitigar o risco	RS.CO-1	Intermédio
3	2	6	Mitigar o risco	RS.CO-2	Intermédio
3	2	6	Mitigar o risco	RS.CO-3	Intermédio
3	2	6	Mitigar o risco	RS.CO-4	Intermédio
3	2	6	Mitigar o risco	RS.CO-5	Intermédio
3	2	6	Mitigar o risco	RS.AN-1	Intermédio
3	1	3	Mitigar o risco	RS.AN-2	Básico
3	1	3	Mitigar o risco	RS.AN-3	Intermédio
2	2	4	Mitigar o risco	RS.AN-4	Intermédio
2	2	4	Mitigar o risco	RS.AN-5	Básico
3	2	6	Mitigar o risco	RS.MI-1	Intermédio
3	2	6	Mitigar o risco	RS.MI-2	Intermédio
3	1	3	Mitigar o risco	RS.MI-3	Básico
3	2	6	Mitigar o risco	RS.ME-1	Avançado
2	2	4	Mitigar o risco	RS.ME-2	Intermédio
3	2	6	Mitigar o risco	RC.PR-1	Intermédio
3	2	6	Mitigar o risco	RC.ME-1	Avançado
3	2	6	Mitigar o risco	RC.ME-2	Intermédio
3	2	6	Mitigar o risco	RC.CO-1	Intermédio
3	2	6	Mitigar o risco	RC.CO-2	Intermédio

Tabela 15 - Análise de risco

A análise do risco teve em consideração a natureza do negócio bem como as considerações definidas na secção 3.3 *Metodologia de gestão de risco*.

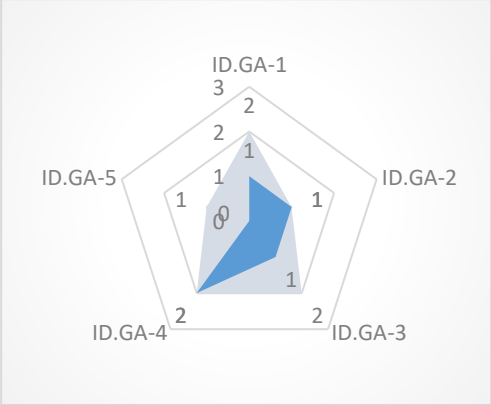
4.3 Identificação e priorização de lacunas (Passo 6)

O Passo 6 refere-se à identificação e priorização de lacunas entre o grau de maturidade atual e o grau de maturidade desejado para cada subcategoria do QNRCS.

4.3.1 Gestão de ativos (ID.GA)

A organização deve identificar os dados, colaboradores, equipamentos, sistemas e instalações que permitem cumprir os seus objetivos no decorrer da sua atividade. Devem ser identificados e geridos de forma consistente com aquela que é a sua relevância no cumprimento dos objetivos da organização e com a estratégia de gestão do risco [1].

Pontuação	5 / 8	
Objetivo	Atual	Alvo
ID.GA-1	Básico	Intermédio
ID.GA-2	Básico	Básico
ID.GA-3	Básico	Intermédio
ID.GA-4	Intermédio	Intermédio
ID.GA-5	----------	Básico



Implementação necessária para colmatar as lacunas de maturidade:

ID.GA-1: Os ativos devem ser registados sistematicamente com informação completa e pertinente a cada ativo;
ID.GA-1: Os ativos devem ser identificados individualmente na organização;
ID.GA-1: A cada ativo deve corresponder a associação de um único responsável;
ID.GA-1: Deve existir uma política formalmente divulgada de inventário dos ativos;
ID.GA-3: Os ativos de redes de comunicações devem ser identificados e inventariados;
ID.GA-3: A topologia de rede é registada com identificação de zonas, endereços IP e identificação de ativos críticos;
ID.GA-3: Identificação do fluxo de comunicação entre os sistemas internos e externos;
ID.GA-3: Existência de uma política de procedimentos que definam regras de inventários de redes e fluxos.
ID.GA-5: Os ativos necessários para a prestação de bens e serviços devem ser classificados, mesmo que de forma ad hoc.

O salto do perfil atual para o perfil alvo passará apenas por melhorar alguns processos. Não há a necessidade de implementar uma solução exaustiva de inventário de ativos. O recurso a aplicações de negócio e ficheiros Excel, permitem responder com eficácia aos objetivos desta

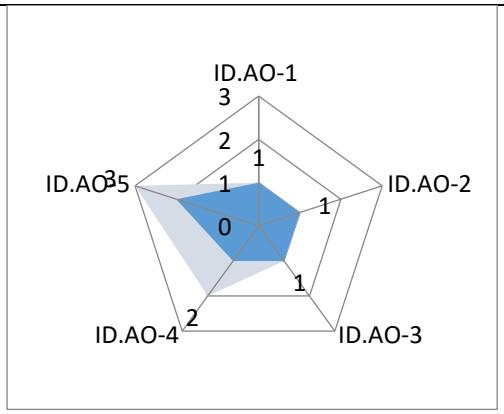
subcategoria. Do ponto de vista processual, o processo beneficiará de um procedimento mais metódico de inventariação e documentação mais atualizada.

Sempre que possível a organização deverá inventariar não apenas os seus ativos, como também os ativos externos que sejam críticos para o negócio (exemplo: redes externas, fornecedores, cadeia logística, etc..). Cada ativo deve ser inventariado, identificando sempre o seu responsável e classificando-o de acordo com a sua criticidade. A descrição dos ativos também é fundamental, pelo que dispositivos físicos e sistemas devem ser inventariados com um número de inventário, nome do equipamento, número de série e localização; enquanto que dispositivos de rede deverão ainda conter o endereço MAC e IP, para além de estarem mapeados em esquemas de rede (referindo a sua topologia). Por fim, e a título de inventariação, os responsáveis dos dispositivos e sistemas devem ser identificados com, pelo menos, o seu nome, contacto e departamento. Os critérios usados para a classificação de ativos de acordo com a criticidade devem ser definidos com recurso ao processo de gestão de risco e descritos na política de gestão de ativos.

4.3.2 Ambiente da Organização (ID.AO)

A organização compreende e prioriza a sua missão, os seus objetivos, as partes interessadas e as suas atividades. Esta informação é utilizada para identificar os papéis e responsabilidades no contexto da cibersegurança e a tomada de decisões no âmbito da gestão dos riscos [1].

Pontuação	6 / 8	
Objetivo	Atual	Alvo
ID.AO-1	Básico	Básico
ID.AO-2	Básico	Básico
ID.AO-3	Básico	Básico
ID.AO-4	Básico	Intermédio
ID.AO-5	Intermédio	Avançado



Implementação necessária para colmatar as lacunas de maturidade:

ID.AO-4: Os ativos que suportam os processos críticos devem ser identificados em sistema de gestão de ativos consolidado;
ID.AO-4: Deve ser utilizada uma ferramenta/aplicação para a gestão integrada dos ativos da organização;
ID.AO-4: A capacidade produtiva dos ativos de infraestrutura, redes e sistemas deve ser registada e monitorizada de modo a garantir a operação.
ID.AO-5: O plano de continuidade deve ser revisto regularmente;
ID.AO-5: Agentes externos em cadeia crítica da organização devem ser auditados quanto às suas capacidades no atendimento à resiliência da organização;

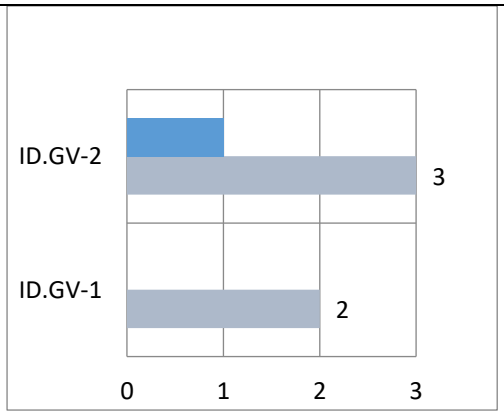
Apesar de existirem redundâncias e testes de resposta e recuperação dos ativos mais críticos, os mesmos não são efetuados de forma sistematizada. O salto do perfil atual para o perfil alvo exige apenas o melhoramento de alguns processos, tais como:

a. A revisão do plano de continuidade: esta revisão tem a tendência de ser revista de forma ad hoc. Fará sentido rever o plano no enquadramento da revisão do Risco. Esta revisão deverá contar com a colaboração dos agentes externos, nomeadamente dos fornecedores e dos próprios clientes.
b. A organização separa ativos da operação dos ativos de suporte, pelo que cada um possui uma aplicação / ferramenta de gestão dedicada. No entanto, uma política de gestão de ativos pode otimizar e sistematizar o processo de inventariação.

4.3.3 Governação (ID.GV)

A organização entende as políticas, processos e procedimentos para gerir e monitorizar as responsabilidades regulamentares, legais, de risco, ambientais e operacionais. Estas políticas, processos e procedimentos contribuem para a sensibilização e consolidação do conhecimento por parte dos órgãos de gestão, tendo em vista a identificação dos riscos no contexto da cibersegurança [1].

Pontuação	1 / 5	
Objetivo	Atual	Alvo
ID.GV-1	----------	Intermédio
ID.GV-2	Básico	Avançado



Implementação necessária para colmatar as lacunas de maturidade:

ID.GV-1: Existência de uma política de segurança estabelecida e divulgada internamente.
ID.GV-1: Os colaboradores são informados e participam em ações de sensibilização sobre a existência da política e os seus termos.
ID.GV-2: Deve-se analisar o impacto que a publicação de novos diplomas legais aplicáveis traz à organização;
ID.GV-2: Deve-se estabelecer uma equipa específica para dar cumprimento às leis e regulamentações aplicáveis;
ID.GV-2: Auditorias e comités internos de tratamento dos controlos de privacidade.

Á dimensão da organização visada, fará sentido atribuir as responsabilidades da cibersegurança (e segurança de informação em geral) a um único responsável. Este

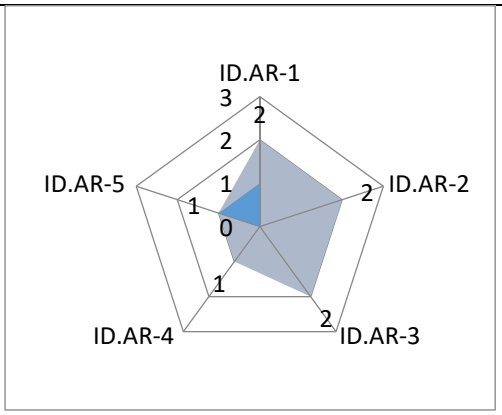
responsável assumirá o papel de CISO[20], cujas funções se encontram descritas no capítulo seguinte[21].

A política de segurança pode definir os princípios da segurança de informação da organização, sustentando-os na sua missão e valores. A implementação e divulgação de uma política de segurança de informação colmatará as restantes as lacunas remanescentes desta categoria do QNRCS. Mais informação acerca da criação da política de segurança de informação pode ser consultada no capítulo seguinte[22].

4.3.4 Avaliação do risco (ID.AR)

A organização tem noção dos riscos de cibersegurança no âmbito da sua atividade (incluindo missão, funções, imagem ou reputação), ativos organizacionais e pessoas.

Pontuação	2 / 8	
Objetivo	Atual	Alvo
ID.AR-1	Básico	Intermédio
ID.AR-2	----------	Intermédio
ID.AR-3	----------	Intermédio
ID.AR-4	----------	Básico
ID.AR-5	Básico	Básico



Implementação necessária para colmatar as lacunas de maturidade:

ID.AR-1: As vulnerabilidades devem ser identificadas e tipificadas nos ativos de informação;
ID.AR-1: Deve existir um processo de gestão de vulnerabilidades que monitoriza os ativos, de acordo com as suas vulnerabilidades atuais e novas;
ID.AR-1: Devem existir uma equipa dedicada ao acompanhamento de publicações de novas vulnerabilidades.
ID.AR-2: Devem existir canais de comunicação estabelecidos com grupos de interesse, sobre ameaças e temas de segurança da informação;
ID.AR-2: Devem ser identificados responsáveis pela comunicação das vulnerabilidades com os grupos de interesse.
ID-AR-3: Deve existir um mapa de ameaças conhecidas, associado a cada tipo de ativo;
ID-AR-3: Deve existir uma indicação de tratamento de cada ameaça mapeada.
ID-AR-4: Deve existir uma metodologia de gestão do risco estabelecida.

[20] Chief Information Officer
[21] Capítulo V – Considerações Gerais, 5.1 CISO- Chief Information Officer
[22] Capítulo V – Considerações Gerais, 5.2 Elaboração e divulgação de uma Política Geral de Segurança de Informação

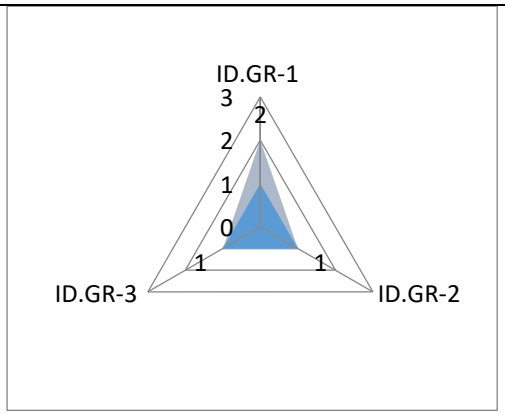
A organização visada possui um processo de avaliação de risco deficiente. Contudo, a implementação de um processo de avaliação de risco disciplinado, alinhado com os pressupostos definidos em 3.4 cobrirá a maioria dos requisitos em falta.

É de acrescentar que para o caso específico da empresa visada, a mesma pode e deverá recorrer a parceiros (dentro da sua área de atividade) para se alimentar de informação relativamente a ameaças e vulnerabilidades. Adicionalmente, existem organizações nacionais que servem este propósito, nomeadamente no que se refere à cibersegurança, como é o caso da Rede CSIRT ou o CNCS.

4.3.5 Estratégia de Gestão de Risco (ID.GR)

Devem ser estabelecidas as prioridades, restrições, níveis de tolerância ao risco e assunções que são utilizadas para suportar a tomada de decisão, no âmbito da gestão do risco operacional.

Pontuação	3 / 4	
Objetivo	Atual	Alvo
ID.GR-1	Básico	Intermédio
ID.GR-2	Básico	Básico
ID.GR-3	Básico	Básico



Implementação necessária para colmatar as lacunas de maturidade:

ID.GR-1: As vulnerabilidades devem ser identificadas e tipificadas nos ativos de informação;
ID.GR-1: Deve existir um processo de gestão de vulnerabilidades que monitoriza os ativos, de acordo com as suas vulnerabilidades atuais e novas;
ID.GR-1: Deve existir uma equipa dedicada ao acompanhamento de publicações de novas vulnerabilidades.

Para colmatar esta lacuna, dever-se-á adotar um processo regular de identificação de vulnerabilidades. Face à dimensão da organização visada, este processo contará com:

1. Consulta regular de *feeds* e grupos de interesse com o propósito de alimentação de informação acerca de vulnerabilidades;
2. Implementação de uma VM[23] com Kali Linux instalado, com OpenVAS[24] e Nikto[25].

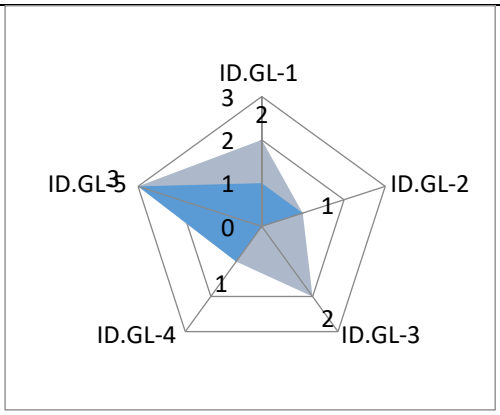
[23] Virtual Machine (Máquina Virtual)
[24] Ferramenta gratuita de aferição de vulnerabilidades de infraestrutura [15]
[25] Ferramenta gratuita de aferição de vulnerabilidades de aplicações Web [16]

O processo de identificação de vulnerabilidades a implementar encontra-se descrito mais detalhadamente no capítulo seguinte[26]. Relativamente à alimentação de *feeds*, o mesmo processo encontra-se também descrito no próximo capítulo[27].

4.3.6 Gestão do risco da cadeia logística (ID.GL)

Devem ser estabelecidas as prioridades, restrições, níveis de tolerância ao risco e assunções que são utilizadas para suportar a tomada de decisão, no âmbito da gestão do risco operacional da cadeia logística. A organização deve estabelecer e implementar os processos para identificar, avaliar e gerir os riscos inerentes à cadeia logística.

Pontuação	6 / 9	
Objetivo	Atual	Alvo
ID.GL-1	Básico	Intermédio
ID.GL-2	Básico	Básico
ID.GL-3	----------	Intermédio
ID.GL-4	Básico	Básico
ID.GL-5	Avançado	Avançado



Implementação necessária para colmatar as lacunas de maturidade:

ID.GL-1: A organização deve aplicar a gestão de riscos na sua cadeia logística.
ID.GL-3: A organização deve garantir que o tema da segurança da informação é incluído nos contratos da cadeia logística;
ID.GL-3: A política de fornecedores deve incluir controlos de segurança na cadeia logística.

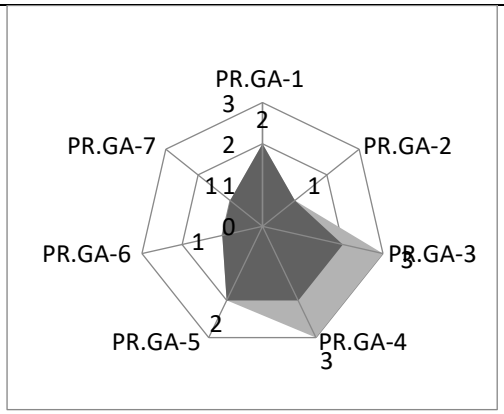
Para colmatar a lacuna associada a esta categoria do QNRCS, bastará incluir os riscos associados à cadeia logística na matriz de gestão de risco. Qualquer controlo de mitigação associada ao risco de fornecedores ou parceiros deve ser descrita na política de segurança da cadeia logística.

4.3.7 Gestão de Identidades, Autenticação e Controlo de Acessos (PR.GA)

Os acessos aos ativos físicos, lógicos e às instalações associadas, devem ser limitados às pessoas, processos e equipamentos autorizados. Estes devem ser geridos de acordo com a avaliação do risco de acesso não autorizado [1].

[26] Capítulo V – Considerações Gerais, 5.4 Gestão de Vulnerabilidades
[27] Capítulo V – Considerações Gerais, 5.3 Fonte de informação e ameaças e risco

Pontuação	11 / 13	
Objetivo	Atual	Alvo
PR.GA-1	Intermédio	Intermédio
PR.GA-2	Básico	Básico
PR.GA-3	Intermédio	Avançado
PR.GA-4	Intermédio	Avançado
PR.GA-5	Intermédio	Intermédio
PR.GA-6	Básico	Básico
PR.GA-7	Básico	Básico



Implementação necessária para colmatar as lacunas de maturidade:

PR.GA-3: Bloqueios proativos contra acessos remotos não autorizados;
PR.GA-3: Autenticação federada aos demais sistemas da organização;
PR.GA-3: Autenticação com multi-fatores para acessos remotos;
PR.GA-3: Monitorização dos acessos remotos;
PR.GA-3: Revisão regular dos acessos e tráfego.
PR.GA-4: A definição de funções e níveis de acessos são revistos regularmente;
PR.GA-4: Os acessos concedidos com privilégios elevados são revistos regularmente;
PR.GA-4: Os acessos são monitorizados ao pormenor;
PR.GA-4: Existem controlos complementares para os acessos elevados, tais como férias obrigatórias e job rotation;
PR.GA-4: Utilizadores com acessos elevados são submetidos a controlos suplementares.

A organização possui a sua infraestrutura de TI segmentada, em serviços de suporte e operação. A maior parte das lacunas situa-se na infraestrutura de suporte.

A autenticação federada pode ser garantida através da implementação de uma máquina virtual com Windows Server ou alternativamente, ZenTyal[28] (a versão Linux equivalente ao Windows Server). Adicionalmente, a implementação de um processo de monitorização das ligações VPN, bem como de acessos aplicacionais já são efetuados, mas de forma reativa; pelo que a melhoria deste processo será suficiente para preencher as lacunas.

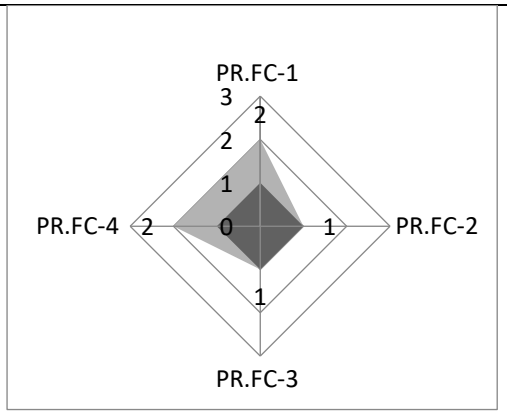
Por fim, deve ser implementado um processo rigoroso de revisão de acessos, sobretudo na sua infraestrutura de operação, que pode ser alcançada através da revisão manual de credenciais de acesso.

[28] Para mais detalhe relacionado com o tema de implementação de sistemas de gestão de acesso, consultar Capítulo V – Considerações Gerais, 5.5 Gestão de Acessos.

4.3.8 Formação e sensibilização (PR.FC)

Devem ser ministradas sessões de sensibilização em cibersegurança a colaboradores e fornecedores. Estes, devem ser formados para cumprirem as suas responsabilidades e os seus deveres relacionados com a cibersegurança, em concordância com as políticas, processos, procedimentos e acordos relevantes [1].

Pontuação	4 / 6	
Objetivo	Atual	Alvo
PR.FC-1	Básico	Intermédio
PR.FC-2	Básico	Básico
PR.FC-3	Básico	Básico
PR.FC-4	Básico	Intermédio



Implementação necessária para colmatar as lacunas de maturidade:

PR.FC-1: As ações de formação e consciencialização devem ser registadas em planos, procedimentos e metas da organização;
PR.FC-1: As formações devem ser planeadas consoante a audiência.
PR.FC-4: Os papéis e responsabilidades da gestão de topo no âmbito da segurança da informação devem ser estabelecidos.

Tipicamente, o vetor de ataque mais comum às organizações é o fator humano. Por este motivo, uma boa consciencialização da temática de cibersegurança e segurança de informação pode revelar-se mais eficaz do que qualquer outra implementação técnica, quer do ponto de vista de eficiência, quer na ótica da relação eficácia/custo.

Neste sentido, um plano de formações técnicas, processuais e comportamentais de caráter periódico deve ser adotado. Este plano pode ser elaborado recorrendo a um conjunto de conteúdos gratuitos disponíveis online (ex: CNSC[29]), ou à criação de conteúdos próprios. Alternativamente, poder-se-á recorrer a formações online de caráter mais técnico de baixo custo (ex: Udemy ou Cybrary) ou até mesmo a serviços de formação. A operacionalização das formações / ações de sensibilização é abordada no próximo capítulo[30].

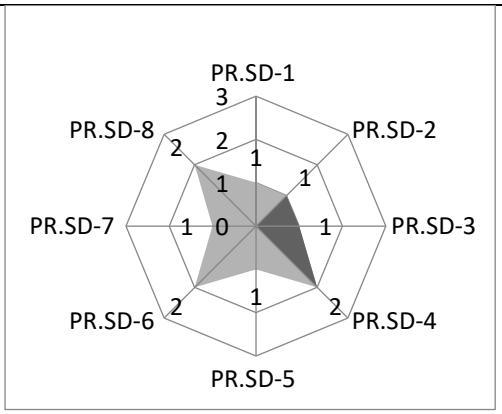
Assim, no caso da PME visada, a implementação de um processo diligente de sensibilização para o tema da segurança de informação e cibersegurança, atualizada mensalmente é a resposta mais adequada à sua realidade.

[29] Boas práticas do CNCS - https://dyn.cncs.gov.pt/pt/boaspraticas/
[30] Capítulo V – Discussão, 5.11 Formação e Sensibilização

4.3.9 Segurança de dados (PR.SD)

Os acessos aos ativos físicos, lógicos e às instalações associadas, devem ser limitados às pessoas, processos e equipamentos autorizados. Estes devem ser geridos de acordo com a avaliação do risco de acesso não autorizado [1].

Pontuação	8 / 11	
Objetivo	Atual	Alvo
PR.SD-1	----------	Básico
PR.SD-2	Básico	Básico
PR.SD-3	Básico	Básico
PR.SD-4	Intermédio	Intermédio
PR.SD-5	----------	Básico
PR.SD-6	Intermédio	Intermédio
PR.SD-7	----------	Básico
PR.SD-8	Intermédio	Intermédio



Implementação necessária para colmatar as lacunas de maturidade:

PR.SD-1: Devem ser estabelecidas regras de proteção da confidencialidade, integridade e disponibilidade dos ficheiros, documentos e dados.
PR.SD-7: A segregação de ambientes deve ser efetuada.

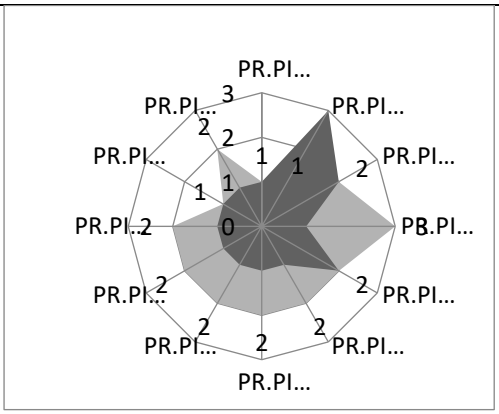
A colmatação destas lacunas é assegurada através da:

1. implementação de uma máquina virtual simulando o ambiente de produção, sem os dados de produção, para garantir uma segregação de ambientes;
2. adotar uma política de classificação de informação que estabeleça as regras de manuseamento de ficheiros, quer em formato digital, quer em formato físico.

4.3.10 Procedimentos e processos de proteção da informação (PR.PI)

As políticas de segurança, processos e procedimentos devem ser mantidas e utilizadas por forma a permitir gerir a proteção das redes e sistemas de informação [1].

Pontuação	16 / 22	
Objetivo	Atual	Alvo
PR.PI-1	Básico	Básico
PR.PI-2	N/A	Básico
PR.PI-3	Intermédio	Intermédio
PR.PI-4	Básico	Avançado
PR.PI-5	Intermédio	Intermédio
PR.PI-6	Básico	Intermédio
PR.PI-7	Básico	Intermédio
PR.PI-8	Básico	Intermédio
PR.PI-9	Básico	Intermédio
PR.PI-10	Básico	Intermédio
PR.PI-11	Básico	Básico
PR.PI-12	Básico	Intermédio



Implementação necessária para culmatar as lacunas de maturidade:

PR.PI-4: Devem ser estabelecidas regras internas formais para a realização das cópias de segurança;

PR.PI-4: A integridade das cópias de segurança deve ser verificada de forma independente em relação ao ambiente protegido.

PR.PI-4: Os procedimentos realizados para as cópias de segurança devem ser verificados.

PR.PI-6: A informação sensível é destruída apropriadamente quando já não for necessária;

PR.PI-6: Devem ser documentados procedimentos de destruição de informação sigilosa.

PR.PI-7: Devem ser estabelecidos procedimentos e controlos de monitorização e melhoria contínua.

PR.PI-8: A eficácia das tecnologias de proteção deve ser medida e avaliada;

PR.PI-8: Deve existir um processo estabelecido de evolução através de lições aprendidas.

PR.PI-9: Devem existir processos, formalmente definidos, para as atividades relativas a resposta a incidentes e garantia da resiliência da organização;

PR.PI-9: Os planos de resposta devem ser medidos e avaliados quando executados.

PR.PI-10: Os planos de continuidade devem ser registados e testados quanto ao âmbito definido.

PR.PI-12: As vulnerabilidades devem ser identificadas com equipas de tratamento adequadas;

PR.PI-12: A análise de vulnerabilidades deve ser regular e sistemática;

PR.PI-12: As vulnerabilidades devem ser exploradas, para atestar o seu nível de risco real.

Esta categoria revela-se uma das mais trabalhosas para implementar. Para endereçar o tema de:

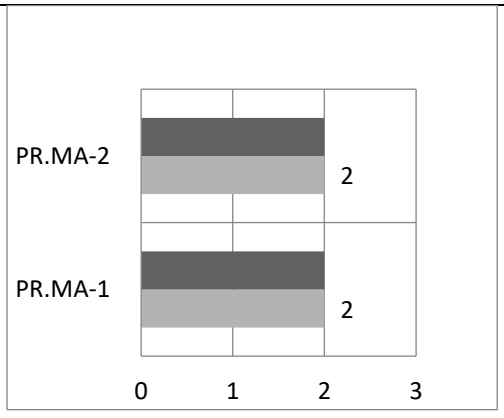
1. **cópias de segurança**: bastará implementar um processo de backup aos ficheiros que ainda não são alvo de backup regular, nomeadamente os ficheiros de *fileshare*. Face à cadência de escrita, justifica-se apenas colocar um procedimento de cópia no NAS para outro disco, com recorrência semanal – para backups totais – e diárias – backups incrementais e com tempo de retenção de três semanas.
2. **manuseamento de documentos**: a implementação de uma política de classificação de informação com a descrição do manuseamento dos documentos (reprodução, transporte, transferência e destruição) de acordo com a sua classificação, será suficiente.
3. **gestão de lições aprendidas**: a organização estabelece um procedimento de lições aprendidas por cada incidente de segurança identificado. Face ao reduzido tamanho da organização, este procedimento pode ficar a cargo do responsável pela gestão de risco. Neste procedimento deve caber a avaliação dos planos de resposta quando os mesmos são executados.
4. **planos de continuidade de negócio**: apesar de os planos de continuidade de negócio existirem, os mesmos devem ser testados com regularidade. Para o efeito, bastará estabelecer um procedimento para teste do plano já em vigor. Face à dimensão da organização, a responsabilidade de se implementar este procedimento pode incidir sobre o responsável pela gestão de risco.
5. **gestão de vulnerabilidades**: tal como falado anteriormente, a implementação da gestão de vulnerabilidades (descrito na categoria 4.1.5 Estratégia de Gestão de Risco) deverá ser acompanhada pelo processo de tratamento, articulado com o processo de gestão de risco.

4.3.11 Manutenção (PR.MA)

A manutenção e reparação das redes e sistemas de informação deve ser realizada em concordância com as políticas, processos e procedimentos instituídos.

Pontuação	4 / 4	
Objetivo	Atual	Alvo
PR.MA-1	Intermédio	Intermédio
PR.MA-2	Intermédio	Intermédio

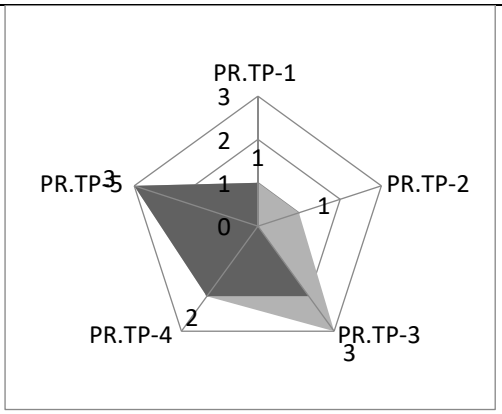
Nada a reportar.



4.3.12 Tecnologia de proteção (PR.TP)

As soluções técnicas de segurança devem ser geridas por forma a garantir a confidencialidade, integridade e disponibilidade das redes e sistemas de informação, em concordância com as políticas relacionadas, processos, procedimentos e acordos relevantes [1].

Pontuação	8 / 10	
Objetivo	Atual	Alvo
PR.TP-1	Básico	Básico
PR.TP-2	----------	Básico
PR.TP-3	Intermédio	Avançado
PR.TP-4	Intermédio	Intermédio
PR.TP-5	Avançado	Avançado



Implementação necessária para colmatar as lacunas de maturidade:

PR.TP-2: Deve existir uma implementação mínima de medidas de proteção aos suportes de dados amovíveis.
PR.TP-3: Os acessos devem ser condizentes com as necessidades mínimas para as funções.

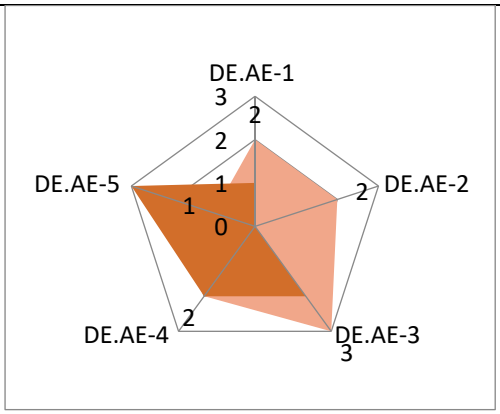
A fim de alcançar a maturidade alvo, bastará:

1. implementar um processo de limpeza de dispositivos amovíveis cada vez que se efetuar transferência de ficheiros através dos mesmos. Os dispositivos amovíveis também devem ser encriptados e acessíveis através de chave, pelo que esta medida pode ser alcançada através das opções de Bitlocker disponíveis no Windows 10.
2. implementar um processo de revisão de acessos às aplicações de negócio e redes da organização, preferencialmente com periodicidade máxima de 180 dias.

4.3.13 Anomalias e eventos (DE.AE)

Devem ser detetadas as atividades anómalas em tempo útil, bem como deve ser assegurada a compreensão do impacto potencial dos eventos [1].

Pontuação	4 / 10	
Objetivo	Atual	Alvo
DE.AE-1	Intermédio	Intermédio
DE.AE-2	Básico	Intermédio
DE.AE-3	Básico	Avançado
DE.AE-4	----------	Intermédio
DE.AE-5	----------	Básico



Implementação necessária para colmatar as lacunas de maturidade:

DE.AE-2: As tentativas de ataques e incidentes de segurança devem ser detetadas;
DE.AE-2: Deve ser estabelecido o tratamento apropriado de incidentes de segurança;
DE.AE-2: Deve ser realizada a comunicação apropriada de incidentes com as partes interessadas.
DE.AE-3: Os eventos de segurança devem ser geridos e analisados;
DE.AE-3: Devem ser considerados eventos de diversas fontes internas e externas.
DE.AE-3: Deve existir melhoria contínua dos controlos, a partir do tratamento de eventos anteriores;
DE.AE-3: Devem ser estabelecidos mecanismos de controlo de um evento de segurança nas suas infraestruturas.
DE.AE-4: Os eventos de segurança devem ser classificados conforme o seu impacto percebido.
DE.AE-4: Deve ser estabelecido um processo de gestão de eventos;
DE.AE-4: Os efeitos do impacto de um evento devem ser aferidos.
DE.AE-5: Os incidentes devem ser abertos sem limite formal definido para o número de eventos relacionados.

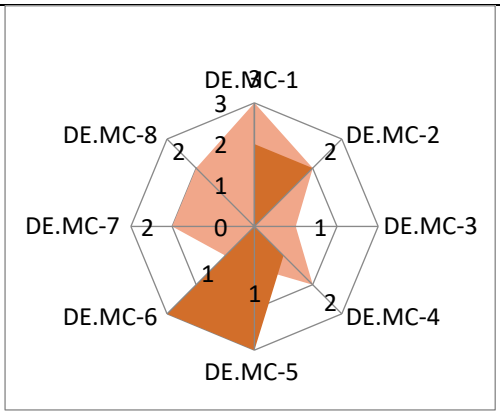
A fim de dar resposta às necessidades da categoria DE.AE, a organização deverá instalar um SIEM. Tendo em conta a dimensão da organização e os recursos disponíveis, a organização instalará uma VM com Graylog (SIEM *opensource*). No caso em particular da organização visada, o seu processo de monitorização de eventos de segurança de informação deverá ser externalizado. O processo de gestão de eventos deve ser definido pela organização (criticidade dos eventos, planos de ação, e comunicação) e articulado com a entidade prestadora do serviço de monitorização. Para mais detalhe relativamente à implementação de um SOC e tipos de SIEM, consultar o capítulo seguinte[31].

[31] Capítulo V – Discussão 5.8. SOC, 5.7 SIEM

4.3.14 Monitorização Contínua de Segurança (DE.MC)

As redes e sistemas de informação devem ser monitorizadas para identificação de eventos de cibersegurança e verificação da eficácia das medidas de proteção aplicadas [1].

Pontuação	11 / 18	
Objetivo	Atual	Alvo
DE.MC-1	Intermédio	Avançado
DE.MC-2	Intermédio	Intermédio
DE.MC-3	----------	Básico
DE.MC-4	Básico	Intermédio
DE.MC-5	N/A	N/A
DE.MC-6	N/A	N/A
DE.MC-7	----------	Intermédio
DE.MC-8	----------	Intermédio



Implementação necessária para colmatar as lacunas de maturidade:

DE.MC-1: Deve ser realizada a associação de eventos de segurança de origens distintas;
DE.MC-1: Os acessos a ativos conhecidos devem ser restringidos;
DE.MC-1: A gestão de incidentes deve ser suportada por uma equipa dedicada.
DE.MC-3: A atividade dos colaboradores deve ser monitorizada;
DE.MC-3: Os incidentes devem ser detetados manualmente.
DE.MC-4: Estão estabelecidas regras formais de avaliação de códigos maliciosos;
DE.MC-4: As verificações periódicas de códigos maliciosos devem ser realizadas periodicamente.
DE.MC-7: Os acessos devem ser monitorizados e analisados manualmente
DE.MC-7: Os pedidos de acesso às infraestruturas e servidores devem ser monitorizados;
DE.MC-7: Os dados dispersos devem ser recolhidos e centralizados para análise de anomalias.
DE.MC-8: A pesquisa por vulnerabilidades nos sistemas e redes de comunicação deve ser feita
DE.MC-8: As vulnerabilidades identificadas nos sistemas e redes de comunicação devem ser analisadas regularmente.

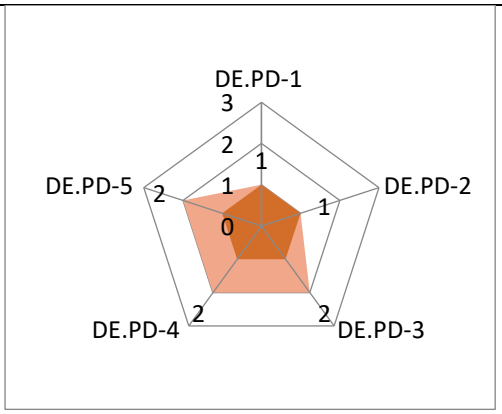
Conforme indicado na categoria anterior, a externalização do SOC permite ter uma equipa dedicada à monitorização de eventos. O SIEM monitorizará as atividades dos utilizadores, só e nomeadamente os acessos a redes e sistemas da organização.

O processo de pesquisa de vulnerabilidades será efetuado de forma regular (prevista conforme o descrito no capítulo seguinte[32]), prevendo o uso de ferramentas *opensource* já mencionadas anteriormente (PR.PI e ID.GR). O processo de gestão de vulnerabilidades é articulado com o processo de gestão de eventos de segurança, sendo os mesmos geridos pelo responsável pela gestão de risco.

4.3.15 Processos de Deteção (DE.PD)

Os processos de deteção e respetivos procedimentos devem ser mantidos e testados para garantir o reconhecimento de eventos anómalos [1].

Pontuação	5 / 8	
Objetivo	Atual	Alvo
DE.PD-1	Básico	Básico
DE.PD-2	Básico	Básico
DE.PD-3	Básico	Intermédio
DE.PD-4	Básico	Intermédio
DE.PD-5	Básico	Intermédio



Implementação necessária para colmatar as lacunas de maturidade:

DE.PD-3: Deve existir um processo sistemático de analise aos processos de deteção;
DE.PD-3: Os processos de deteção devem ser medidos regularmente.
DE.PD-4: Deve ser estabelecido internamente um canal de comunicação adequado;
DE.PD-4: Os incidentes detetados devem ser registados adequadamente.
DE.PD-5: Devem existir mecanismos de medição e avaliação dos processos de deteção.

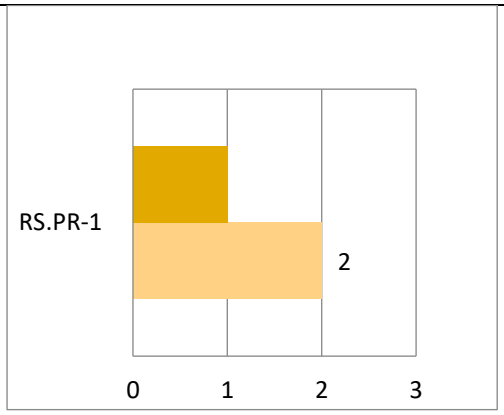
Tendo em conta a dimensão da organização visada, fará sentido incluir o procedimento de revisão dos processos de deteção aquando da revisão e reavaliação do risco de S.I.

4.3.16 Planeamento de resposta (RS.PR)

Os processos de resposta e respetivos procedimentos devem ser executados e mantidos para garantir resposta aos incidentes detetados [1].

[32] Capítulo V – Discussão, 5.4 Gestão de Vulnerabilidades

Pontuação	1 / 2	
Objetivo	Atual	Alvo
RS.PR-1	Básico	Intermédio



Implementação necessária para colmatar as lacunas de maturidade:

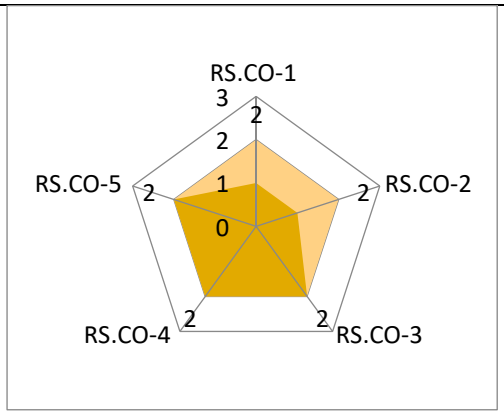
RS.PR-1: Os processos de reposta a incidentes devem ser sistematizados e incluem as fases de contenção e erradicação, bem como a identificação dos diversos responsáveis e o escalonamento.

Para melhor abordar este tema, a organização deve estabelecer um plano formal de resposta a incidentes, no qual indique claramente quais os procedimentos de contenção e erradicação. Este plano apenas pode prever incidentes conhecidos ou previsíveis, dentro dos riscos já identificados pelo processo de gestão de risco.

4.3.17 Comunicações (RS.CO)

As atividades de resposta a incidentes devem ser coordenadas com as partes interessadas.

Pontuação	8 / 10	
Objetivo	Atual	Alvo
RS.CO-1	Básico	Intermédio
RS.CO-2	Básico	Intermédio
RS.CO-3	Intermédio	Intermédio
RS.CO-4	Intermédio	Intermédio
RS.CO-5	Intermédio	Intermédio



Implementação necessária para colmatar as lacunas de maturidade:

RS.CO-1: Os colaboradores devem ter conhecimento sobre os procedimentos e responsabilidades;
RS.CO-1: Devem ser estabelecidos os guiões de resposta a incidentes.
RS.CO-2: A capacidade de reporte de incidentes deve estar garantida;
RS.CO-2: Estão estabelecidos critérios de reporte de incidentes.

Numa organização com a dimensão da organização visada, o processo de reporte interno de incidentes não precisa necessariamente de recorrer a uma aplicação específica para o efeito

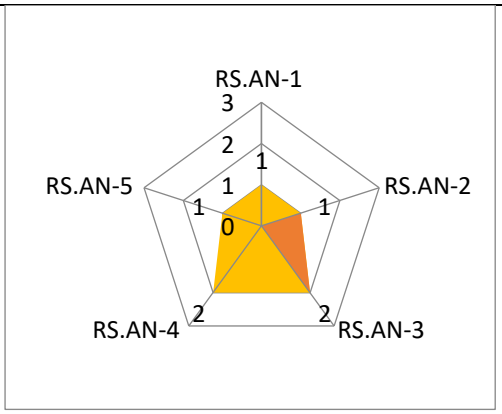
(ex: EasyVista, ServiceDeskPlus, etc), ao contrário de como acontece usualmente numa grande organização[33]. Contudo, é imperativo que os incidentes sejam registados, reportados e articulados com as partes interessadas. Neste sentido, o responsável pela segurança deverá ficar com esta tarefa, criando um processo interno de reporte de incidentes (de identificação de incidentes) e depois de comunicação interna e externa[34].

Estes processos de comunicação devem ser planeados consoante a criticidade do incidente.

4.3.18 Análise (RS.AN)

A análise de incidentes deve ser conduzida de forma a garantir uma resposta efetiva e apoiar as atividades de recuperação.

Pontuação	5 / 8	
Objetivo	Atual	Alvo
RS.AN-1	Básico	Intermédio
RS.AN-2	Básico	Básico
RS.AN-3	Intermédio	Intermédio
RS.AN-4	----------	Intermédio
RS.AN-5	Básico	Básico



Implementação necessária para colmatar as lacunas de maturidade:

RS.AN-1: Deve existir o registo de notificações de eventos elevados a incidentes
RS.AN-1: Devem existir orientações sobre a ativação da gestão de incidentes.
RS.AN-1: Devem ser estabelecidas práticas de acompanhamento aos eventos detetados;
RS.AN-1: Deve existir um plano de resposta a incidentes.
RS.AN-4: Deve ser estabelecida uma taxonomia de categorização de incidentes;
RS.AN-4: A categorização do incidente deve estar presente no momento da resposta.

O processo de análise de incidentes é reativo e com procedimentos de resposta ad hoc. Assim sendo, a organização deve implementar um processo de análise (escrito) que vise agilizar o processo de resposta a incidentes: quer na análise, quer no subsequente acionamento do processo de gestão de incidentes. Este plano não necessita de nenhuma implementação tecnológica para o efeito, mas requer tempo para se definir e escrever.

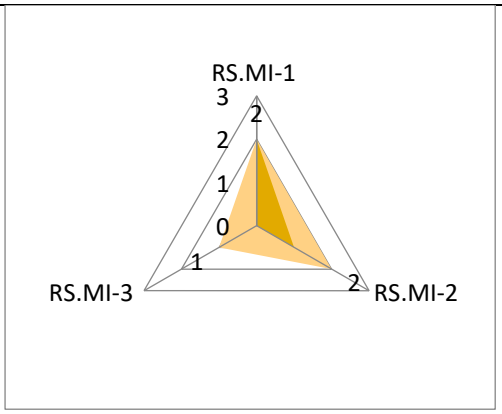
Este plano de resposta deve usar uma taxonomia que lhe permita de forma eficiente categorizar os incidentes e eventos de segurança. Para o efeito, recorrer-se-á à taxonomia da Rede CSIRT [20].

[33] Conforme descrito em Capítulo V Considerações Gerais, 5.12 Reporte de Incidentes
[34] Conforme referido em Capítulo V Considerações Gerais, 5.10.1 Plano de Comunicações

4.3.19 Mitigação (RS.MI)

Devem ser realizadas atividades para conter, mitigar ou resolver um incidente ocorrido [1].

Pontuação	3 / 5	
Objetivo	Atual	Alvo
RS.MI-1	Intermédio	Intermédio
RS.MI-2	Básico	Intermédio
RS.MI-3	----------	Básico



Implementação necessária para colmatar as lacunas de maturidade:

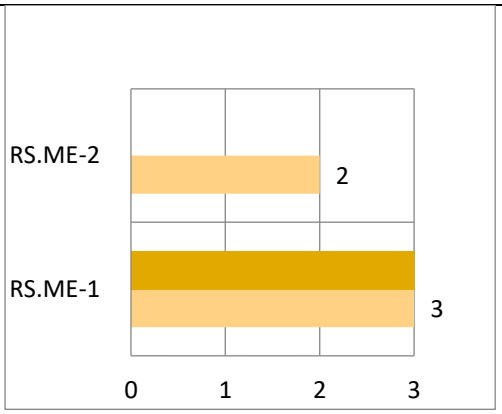
RS.MI-2: Devem ser estabelecidas práticas para a redução do impacto dos incidentes;
RS.MI-2: Os procedimentos sobre o tratamento de incidentes devem ser documentados.
RS.MI-3: O tratamento das vulnerabilidades é avaliado mesmo que de forma não estruturada.

O plano de resposta a incidentes deve incluir soluções de mitigação aos mesmos e deve ser documentado, conforme já referido. Processos de backup[35], redundâncias de sistema, segregação de rede e outras medidas de segurança asseguram a redução de impactos nos incidentes.

O tratamento de vulnerabilidades deve ser avaliado à luz da Gestão de Risco, pelo que, no caso da organização visada, esta avaliação deve ficar a cargo do responsável pela segurança de informação.

4.3.20 Melhorias (RS.ME)

Pontuação	3 / 5	
Objetivo	Atual	Alvo
RS.ME-1	Avançado	Avançado
RS.ME-2	----------	Intermédio



Implementação necessária para colmatar as lacunas de maturidade:

[35] Capítulo V Discussão, 5.7 Política de Backups

RS.ME-2: Os procedimentos devem ser atualizados periodicamente, e não se limitarem às tecnologias e sistemas utilizados

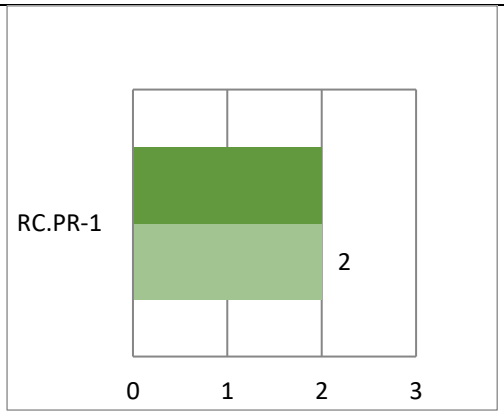
O processo de melhoria dos procedimentos de resposta deve ficar a cargo do responsável de segurança, articulando assim o processo de melhoria e revisão destes planos com o processo de revisão e reavaliação da Gestão de Risco.

4.3.21 Plano de recuperação (RS.PR)

Os processos e procedimentos de recuperação devem ser executados e mantidos para garantir a recuperação das redes e sistemas de informação afetados pelos incidentes [1].

Pontuação	2 / 2	
Objetivo	Atual	Alvo
ID.GA-1	Intermédio	Intermédio

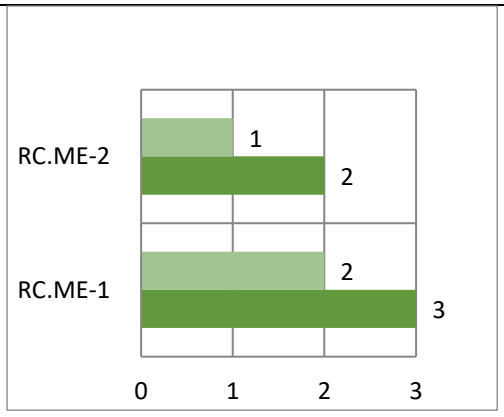
Nada a reportar.



4.3.22 Melhorias (RC.ME)

Os planos e processos de recuperação devem ser melhorados através da incorporação de lições aprendidas, resultantes de incidentes passados e correntes [1].

Pontuação	3 / 5	
Objetivo	Atual	Alvo
RC.ME-1	Intermédio	Avançado
RC.ME-2	Básico	Intermédio



Implementação necessária para colmatar as lacunas de maturidade:

RC.ME-1: Devem ser identificadas as oportunidades de melhoria que possam ser implementadas;
RC.ME-1: Os planos de recuperação devem ser atualizados com as melhorias encontradas.

RC.ME-2: Devem ser estabelecidos procedimentos de revisão e atualização da documentação e dos processos pertinentes à recuperação; **RC.ME-2:** As equipas afetas à recuperação de incidentes devem seridas geridas.

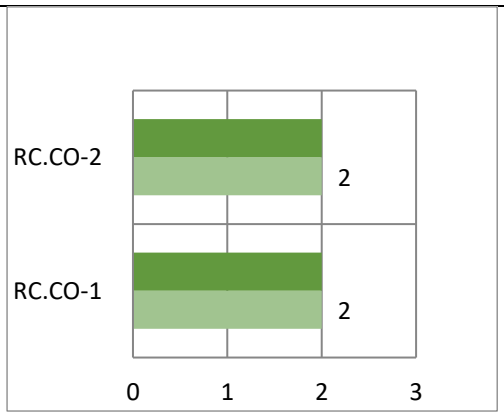
Por forma a simplificar estes procedimentos, a organização articulará a revisão de todos os procedimentos de recuperação com a revisão e com os processos de reavaliação do risco.

4.3.23 Comunicações (RS.CO)

Os planos e processos de recuperação devem ser melhorados através da incorporação de lições aprendidas, resultantes de incidentes passados e correntes [1].

Pontuação	3 / 4	
Objetivo	Atual	Alvo
RC.CO-1	Intermédio	Intermédio
RC.CO-2	Intermédio	Intermédio

Nada a reportar.



4.4 Implementação do plano de ação (Passo 7)

O plano de ação tem em consideração as lacunas e sobretudo as não conformidades, definidas em 3.3. A priorização das atividades terá em conta a severidade das não-conformidades bem como os objetivos que às mesmas pertencem (Identificar, Proteger …), visto que os objetivos são interdependentes, e estruturados de forma a que o quinto objetivo assente na execução do quarto, e o quarto no terceiro, e assim sucessivamente.

Identificação das não-conformidades, conforme especificado em 3.3:

SUBCATEGORIA	RISCO	P. ATUAL	P. ALVO	LACUNA	Tratamento	Não conformidades
ID.GA-1	6	1	2	-1	Mitigar o risco	Não-conformidade média
ID.GA-2	2	1	1	0	Mitigar o risco	Em conformidade
ID.GA-3	3	1	2	-1	Mitigar o risco	Não-conformidade baixa
ID.GA-4	3	2	2	0	Mitigar o risco	Em conformidade
ID.GA-5	4	0	1	-1	Mitigar o risco	Não-conformidade baixa
ID.AO-1	2	1	1	0	Aceitar o risco	Em conformidade
ID.AO-2	2	1	1	0	Aceitar o risco	Em conformidade
ID.AO-3	1	1	1	0	Aceitar o risco	Em conformidade
ID.AO-4	4	1	2	-1	Mitigar o risco	Não-conformidade baixa
ID.AO-5	6	2	3	-1	Mitigar o risco	Não-conformidade média

ID.GV-1	4	0	2	-2	Mitigar o risco	Não-conformidade baixa
ID.GV-2	6	1	3	-2	Mitigar o risco	Não-conformidade alta
ID.AR-1	6	1	2	-1	Mitigar o risco	Não-conformidade média
ID.AR-2	2	0	2	-2	Mitigar o risco	Não-conformidade baixa
ID.AR-3	3	0	2	-2	Mitigar o risco	Não-conformidade baixa
ID.AR-4	3	0	1	-1	Mitigar o risco	Não-conformidade baixa
ID.AR-5	2	1	1	0	Mitigar o risco	Em conformidade
ID.GR-1	4	1	2	-1	Mitigar o risco	Não-conformidade baixa
ID.GR-2	2	1	1	0	Mitigar o risco	Em conformidade
ID.GR-3	2	1	1	0	Aceitar o risco	Em conformidade
ID.GL-1	4	1	2	-1	Mitigar o risco	Não-conformidade baixa
ID.GL-2	2	1	1	0	Mitigar o risco	Em conformidade
ID.GL-3	3	0	2	-2	Mitigar o risco	Não-conformidade baixa
ID.GL-4	2	1	1	0	Mitigar o risco	Em conformidade
ID.GL-5	6	3	3	0	Mitigar o risco	Em conformidade
PR.GA-1	6	2	2	0	Mitigar o risco	Em conformidade
PR.GA-2	4	1	1	0	Mitigar o risco	Em conformidade
PR.GA-3	9	2	3	-1	Mitigar o risco	Não-conformidade média
PR.GA-4	3	2	3	-1	Mitigar o risco	Não-conformidade baixa
PR.GA-5	4	2	2	0	Mitigar o risco	Em conformidade
PR.GA-6	3	1	1	0	Mitigar o risco	Em conformidade
PR.GA-7	3	1	1	0	Mitigar o risco	Em conformidade
PR.FC-1	6	1	2	-1	Evitar o risco	Não-conformidade média
PR.FC-2	4	1	1	0	Mitigar o risco	Em conformidade
PR.FC-3	4	1	1	0	Mitigar o risco	Em conformidade
PR.FC-4	6	1	2	-1	Mitigar o risco	Não-conformidade média
PR.SD-1	4	0	1	-1	Mitigar o risco	Não-conformidade baixa
PR.SD-2	2	1	1	0	Mitigar o risco	Em conformidade
PR.SD-3	2	1	1	0	Mitigar o risco	Em conformidade
PR.SD-4	6	2	2	0	Mitigar o risco	Em conformidade
PR.SD-5	2	0	1	-1	Aceitar o risco	Não-conformidade baixa
PR.SD-6	6	2	2	0	Mitigar o risco	Em conformidade
PR.SD-7	2	0	1	-1	Aceitar o risco	Não-conformidade baixa
PR.SD-8	6	2	2	0	Mitigar o risco	Em conformidade
PR.PI-1	2	1	1	0	Mitigar o risco	Em conformidade
PR.PI-2	4	3	1	2	Evitar o risco	Em conformidade
PR.PI-3	6	2	2	0	Mitigar o risco	Em conformidade
PR.PI-4	6	1	3	-2	Mitigar o risco	Não-conformidade alta
PR.PI-5	6	2	2	0	Mitigar o risco	Em conformidade
PR.PI-6	6	1	2	-1	Mitigar o risco	Não-conformidade média
PR.PI-7	6	1	2	-1	Mitigar o risco	Não-conformidade média
PR.PI-8	6	1	2	-1	Mitigar o risco	Não-conformidade média
PR.PI-9	6	1	2	-1	Mitigar o risco	Não-conformidade média
PR.PI-10	6	1	2	-1	Mitigar o risco	Não-conformidade média
PR.PI-11	1	1	1	0	Aceitar o risco	Em conformidade
PR.PI-12	6	1	2	-1	Mitigar o risco	Não-conformidade média

PR.MA-1	6	2	2	0	Mitigar o risco	Em conformidade
PR.MA-2	6	2	2	0	Mitigar o risco	Em conformidade
PR.TP-1	4	1	1	0	Mitigar o risco	Em conformidade
PR.TP-2	4	0	1	-1	Mitigar o risco	Não-conformidade baixa
PR.TP-3	9	2	3	-1	Mitigar o risco	Não-conformidade média
PR.TP-4	6	2	2	0	Mitigar o risco	Em conformidade
PR.TP-5	6	3	3	0	Mitigar o risco	Em conformidade
DE.AE-1	6	2	2	0	Mitigar o risco	Em conformidade
DE.AE-2	6	1	2	-1	Mitigar o risco	Não-conformidade média
DE.AE-3	6	1	3	-2	Mitigar o risco	Não-conformidade alta
DE.AE-4	6	0	2	-2	Mitigar o risco	Não-conformidade alta
DE.AE-5	3	0	1	-1	Mitigar o risco	Não-conformidade baixa
DE.MC-1	6	2	3	-1	Mitigar o risco	Não-conformidade média
DE.MC-2	6	2	2	0	Mitigar o risco	Em conformidade
DE.MC-3	4	0	1	-1	Mitigar o risco	Não-conformidade baixa
DE.MC-4	6	1	2	-1	Mitigar o risco	Não-conformidade média
DE.MC-5	4	3	1	2	Evitar o risco	Em conformidade
DE.MC-6	3	3	1	2	Evitar o risco	Em conformidade
DE.MC-7	6	0	2	-2	Mitigar o risco	Não-conformidade alta
DE.MC-8	6	0	2	-2	Mitigar o risco	Não-conformidade alta
DE.PD-1	3	1	1	0	Mitigar o risco	Em conformidade
DE.PD-2	3	1	1	0	Mitigar o risco	Em conformidade
DE.PD-3	4	1	2	-1	Mitigar o risco	Não-conformidade baixa
DE.PD-4	6	1	2	-1	Mitigar o risco	Não-conformidade média
DE.PD-5	4	1	2	-1	Mitigar o risco	Não-conformidade baixa
RS.PR-1	6	1	2	-1	Mitigar o risco	Não-conformidade média
RS.CO-1	6	1	2	-1	Mitigar o risco	Não-conformidade média
RS.CO-2	6	1	2	-1	Mitigar o risco	Não-conformidade média
RS.CO-3	6	2	2	0	Mitigar o risco	Em conformidade
RS.CO-4	6	2	2	0	Mitigar o risco	Em conformidade
RS.CO-5	6	2	2	0	Mitigar o risco	Em conformidade
RS.AN-1	4	1	2	-1	Mitigar o risco	Não-conformidade baixa
RS.AN-2	3	1	1	0	Mitigar o risco	Em conformidade
RS.AN-3	3	2	2	0	Mitigar o risco	Em conformidade
RS.AN-4	4	0	2	-2	Mitigar o risco	Não-conformidade baixa
RS.AN-5	4	1	1	0	Mitigar o risco	Em conformidade
RS.MI-1	6	2	2	0	Mitigar o risco	Em conformidade
RS.MI-2	6	1	2	-1	Mitigar o risco	Não-conformidade média
RS.MI-3	3	0	1	-1	Mitigar o risco	Não-conformidade baixa
RS.ME-1	6	3	3	0	Mitigar o risco	Em conformidade
RS.ME-2	4	0	2	-2	Mitigar o risco	Não-conformidade baixa
RC.PR-1	6	2	2	0	Mitigar o risco	Em conformidade
RC.ME-1	6	2	3	-1	Mitigar o risco	Não-conformidade média
RC.ME-2	6	1	2	-1	Mitigar o risco	Não-conformidade média
RC.CO-1	6	2	2	0	Mitigar o risco	Em conformidade
RC.CO-2	6	2	2	0	Mitigar o risco	Em conformidade

Tabela 16 - Aferição da conformidade com o QNRCS

Face aos resultados da tabela acima e tendo em conta os pressupostos definidos nesta tese para a conformidade com o QNRCS (na secção 3.3), conclui-se que a organização não se encontra em conformidade com o QNRCS, como se pode confirmar na tabela seguinte.

Identificar	Em conformidade	11	Responder	Em conformidade	8
	Não-conformidade baixa	10		Não-conformidade baixa	4
	Não-conformidade média	3		Não-conformidade média	4
	Não-conformidade alta	1		Não-conformidade alta	0
Proteger	Em conformidade	22	Recuperar	Em conformidade	3
	Não-conformidade baixa	5		Não-conformidade baixa	0
	Não-conformidade média	10		Não-conformidade média	2
	Não-conformidade alta	1		Não-conformidade alta	0
Detetar	Em conformidade	6	Total	Em conformidade	46
	Não-conformidade baixa	4		Não-conformidade baixa	23
	Não-conformidade média	4		Não-conformidade média	26
	Não-conformidade alta	4		Não-conformidade alta	7

Tabela 17 - Contagem das não-conformidades

Como resulta desta tabela, nenhum dos objetivos do QNRCS se encontra em conformidade, conforme o definido em 3.3. Atendendo ao proposto em 3.5 e 3.6, passa-se a definir o seguinte plano de atividades, para o primeiro ano de implementação[36]:

#Ação	Objetivo	Descrição da ação	Dependentes (da conclusão das ações #)
1	Identificar	Correção das não-conformidades altas	N/A
2		Correção de pelo menos 3 não-conformidades baixas	N/A
3	Proteger	Correção das não-conformidades altas	1;2
4		Correção de pelo menos 2 não-conformidades médias	1;2
5	Detetar	Correção das não-conformidades altas	3;4
6		Correção de pelo menos 1 não-conformidades média	3;4
7	Responder	Correção de pelo menos 1 não-conformidades médias	5;6
8	Recuperar	Correção de pelo menos 2 não-conformidades médias	7;8

Tabela 18 - Priorização de atividades anual

[36] Face aos ciclos de plano de ação, revisão de âmbito e avaliação do risco definidos em 3.5.

Capítulo 5 – Discussão

O capítulo 5 aprofunda alguns processos chave para a gestão da segurança de informação. Mais especificamente, detalha e descreve mais pormenorizadamente processos como o de SOC, CISO e outros temas também abordados no QNRCS que não podem ser ignorados.

5.1 CISO – Chief Information Security Officer

O CISO, Chief Information Security Officer, é uma função exercida na organização, para a qual se estabelece uma relação contratual, com o objetivo de garantir a segurança da informação dessa mesma organização. A criação desta figura não é obrigatória, e para empresas de pequena dimensão, a criação deste posto revela-se um encargo que muitas vezes não conseguem pagar. Acresce ainda que segurança de informação é um tema que abrange muitas áreas, pelo que idealmente o cargo de CISO deverá ser atribuído a uma pessoa que tenha uma visão holística sobre a segurança de informação – técnica, legal e processual. De acordo com o QNRCS, o CISO deve:

- Assegurar a implementação e manter a estratégia de segurança da informação;
- Implementar boas práticas de segurança da informação holísticas e estruturadas;
- Pesquisar, definir e comunicar requisitos de segurança da informação;
- Desenvolver e implementar políticas, processos e procedimentos de segurança da informação;
- Ter conhecimento sobre a legislação e regulamentação específica do setor de atividade da organização;
- Ter conhecimento sobre a legislação e regulamentação referente à segurança de informação;
- Coordenar esforços referentes à proteção de dados pessoais;
- Definir e implementar estratégias de avaliação e de resposta aos riscos;
- Acompanhar e avaliar a execução do processo de gestão de alterações;
- Acompanhar e participar no processo de gestão de incidentes;
- Acompanhar auditorias de segurança e implementação de medidas de melhorias;
- Suportar a organização na estratégia e desempenho e monitorização das tecnologias de informação;
- Dinamizar sessões de sensibilização em segurança da informação e cibersegurança.

Face a tais requisitos, deduz-se facilmente que o encargo de contratar alguém com tais capacidades provavelmente excederá a capacidade financeira normal de uma PME em investimento num novo recurso humano, acrescendo ainda à improbabilidade de contratar, o facto de que este cargo não tergeralmente um impacto direto no negócio. No entanto, tal como os seguros, a segurança é algo que não se vê, mas nota-se a falta dela após um incidente. É por este motivo que o CISO tem um papel fulcral na análise dos temas de segurança de

informação, porque identifica as medidas que possam ser adequadas para implementação na sua organização, não apenas fazendo a ponte com partes interessadas. Garante assim todo o processo de implementação, definição de prioridades e atividades de melhoria contínua, que asseguram que a organização está preparada e adequadamente resiliente em termos de segurança da informação e cibersegurança. Como alternativa à contratação permanente de um recurso para o cargo de CISO, a solução poderá passar pela contratação em modelo de *outsourcing*. A maioria das PMEs, em função da sua dimensão, apresenta uma infraestrutura e complexidade processual relativamente proporcional à sua dimensão. Tendo em mente este facto, várias empresas que atuam na área de consultoria informática disponibilizam um serviço de *CISO-as-a-Service*, no qual uma PME pode contratar um CISO em modelo de consulta *outsourcing*. Este modelo revela-se uma opção mais económica para PMEs, que constituem a maioria do tecido empresarial português.

5.2 Elaboração e divulgação de uma Política Geral de Segurança de Informação

A elaboração de uma Política Geral de Segurança é a pedra basilar da implementação de um Sistema de Gestão de Segurança de Informação. Nela estabelecem-se todas as regras de segurança da organização, passando por políticas, normas, processos, etc… refletindo simultaneamente:

- Estratégia de negócio;
- Regulamentos, legislação e contractos;
- O ambiente atual e as projeções das ameaças à segurança da informação.

Se uma política de segurança necessitar de mais elaboração ou documentação, a mesma deverá constar num documento próprio, e caberá à Política Geral de Segurança remeter o leitor para essa política específica. Ao fim e ao cabo, a Política Geral de Segurança servirá de pivot para todas as outras políticas de segurança. Do mesmo modo, qualquer informação referente a fornecedores, contactos, clientes, e processos da cadeia logística deverá estar contemplada nesta política, devido ao caráter de pivot que esta ela visa ter.

Dada a importância deste documento (e de todos os restantes subjacentes), a política não apenas deverá ser alvo de revisão periódica (para se manter atualizada) como deve ser cumprida do topo à base da hierarquia. Neste sentido, a política está sujeita a aprovação da administração (bem como todas as políticas de segurança subjacentes). A. SANS [19] fornece *templates* para a realização de políticas de segurança de informação

5.3 Fonte de informação de ameaças e risco

O QNRCS recomenda a consulta de fontes de informação de ameaças e risco[37]. Esta recomendação é determinante no papel de "*security awareness*". Atualmente, deparamo-nos com um elevado crescimento e evolução dos ataques informáticos e de engenharia social. A aquisição dos meios técnicos necessários à proteção da informação das organizações é crítica, mas insuficiente na medida que nem sempre acompanha a evolução das ameaças à velocidade que desejaríamos. Acresce ainda que os meios técnicos por si não são suficientes para fazerem frente a ataques de engenharia social, pelo que a melhor defesa para este flagelo passará muito pelo "*security awareness*". Neste sentido, é recomendado que a organização acompanhe na medida do possível as notícias e atualizações sobre ameaças e riscos, escolhendo de preferência fontes confiáveis.

Existem muitas fontes – sites governamentais, revistas de informática, redes sociais, fóruns ou até mesmo a *Dark Web*. Porém, no momento da escolha da fonte, devemos ter em mente:

1. **Informação a mais é o mesmo que pouca informação**: Escolher demasiadas fontes ou *feeds*[38] poderá resultar num excesso de informação que posteriormente não serão exequíveis de ser tratadas ou processadas, o que induz o risco de se desvalorizar a informação que se pode revelar crítica e por conseguinte ir contra o propósito desta medida.
2. **Muitas informações podem não ser verdadeiras**: Toda a informação deve ser filtrada através de pensamento crítico. Porém, nesta área de atuação, o pensamento crítico do tema deverá necessitar de conhecimento técnico vasto, pelo que muitos poderão facilmente ceder a falsas informações ou interpretações erradas da informação disponibilizada.

Dito isto, e à semelhança de outras áreas de domínio da tecnologia (ex: saúde), recomenda-se que se recorra a fontes oficiais ou reconhecidas pela comunidade como credíveis.

Assim, ao leitor português, recomenda-se:

- **Fontes Governamentais**: O CNCS (e autor do QNRCS) assume um papel não apenas pedagógico na medida que efetua variadíssimas recomendações de boas práticas de segurança, como também assume um papel pró-ativo na divulgação de novas ameaças cibernéticas que ameacem o ciberespaço luso[39]. A ENISA é a homóloga

[37] Previsto no QNRCS, no objetivo ID.AR-2 (Categoria Identificar)

[38] Web Feed é um canal direto para fontes de informação como blogs, sites web ou aplicações que alimentam o software de importação de feeds de um utilizador com informação atualizada.

[39] Centro Nacional de Ciber Segurança - https://www.cncs.gov.pt/

europeia do CNCS, pelo que a mesma se afirma como uma excelente fonte oficial de informação útil relativa à segurança de informação[40].

- **Fabricantes de produtos de segurança**: Fornecedores de antivírus como Kaspersky, Symantec ou Avast, e fabricantes de *firewalls* como Checkpoint, Fortinet ou Cisco, desempenham frequentemente um papel de divulgadores de novas ameaças, pelo que seguir alguns destes fabricantes mundialmente conhecidos poder-se-á revelar uma aposta ganhadora.
- **Bases de dados de vulnerabilidades**: Bases de dados de vulnerabilidades são cruciais para o enquadramento de vulnerabilidades conhecidas. Base de dados desta natureza são por exemplo a Common Vulnerability Exposure41 ,a CVE Details42 ou a National Vulnerability Database da NIST43.
- **Outras fontes**: Fontes como revistas de informática e segurança de informação como a Gartner44 poderão revelar-se uma forte aposta para quem procura tendências de mercado, produtos de segurança e relatórios. Numa vertente mais técnica, a comunidade OWASP45 disponibiliza conteúdos sobre boas práticas e disponibiliza informação técnica de segurança como aplicações e investigações de segurança que poderão ser úteis para quem deseja estar na vanguarda do conhecimento da segurança de informação.

É importante referir que existem redes de contactos próprios para partilha de informações de segurança. Tal exemplo é a rede nacional CSIRT[46]. Contudo, face ao âmbito da mesma e às dimensões das organizações visadas nesta tese, será justo afirmar que apesar de benéfico, a adesão à rede por uma micro ou pequena empresa poderá parecer desajustado ou demasiado exigente face às necessidades ou realidade de uma micro ou pequena empresa. Assim, a recomendação deste trabalho académico face a este tema, restringe-se à consulta periódica e/ou configuração de *Web Feeds* e/ou subscrição de *newsletters* das fontes mencionadas

Por fim, é desejável que este processo de obtenção de informação de segurança seja encadeado com outros processos de segurança. Não somente com a gestão de risco, mas também com formações de "security awareness" aos colaboradores e outras partes interessadas ou até mesmo na gestão proactiva de vulnerabilidades.

---

[40] European Union Agency for Ciber Security - https://www.enisa.europa.eu/

[41] https://cve.mitre.org/

[42] https://cve.mitre.org/

[43] https://nvd.nist.gov/

[44] https://www.gartner.com/en

[45] Open Web Application Security Project - https://owasp.org/

[46] Rede Nacional CSIRT - https://www.redecsirt.pt/

Figura 15 - Influências diretas da consulta de fontes de risco e ameaças

5.4 Gestão de Vulnerabilidades

A organização deve rastrear as vulnerabilidades dos seus sistemas periodicamente. Este processo é crucial para a organização ter uma visão sobre a superfície de ataque dos seus ativos e fazer uma correta avaliação do risco associada a esta superfície. Em muitas organizações, este processo é inserido no controlo de qualidade. É neste contexto que as organizações devem definir uma estratégia de avaliação Gestão de Vulnerabilidades. Esta estratégia deve vir definida na Política Geral de Segurança. Esta estratégia deve ser dividida em 3 fases:

1. Identificação das vulnerabilidades
2. Classificação das Vulnerabilidades
3. Tratamento das Vulnerabilidades

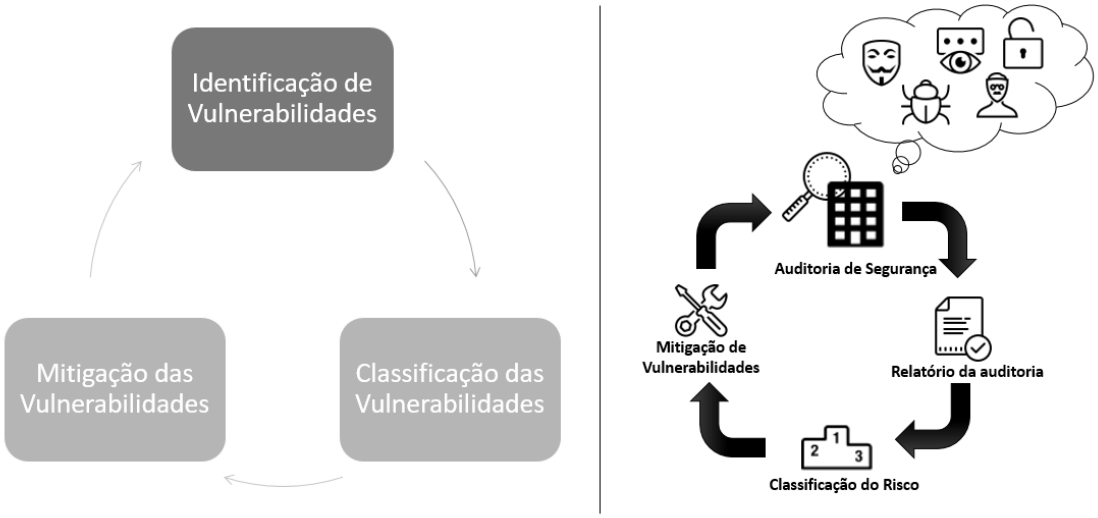


Figura 16 - Processo de Gestão de Vulnerabilidades

Identificação de vulnerabilidades deve acontecer a dois níveis: ao nível de sistemas informáticos e ao nível de processos. Dentro deste tema, existem várias metodologias que dão orientações relativamente à forma de condução de análise de vulnerabilidades, tais como:

- OSSTMM[47] (Open Source Security Testing Methodology Manual)
- OWASP[48] (Open Web Application Security Project)
- NIST[49] (National Institute of Standards and Technology
- PTES[50] (Penetration Testing Methodologies and Standards)

Estas metodologias conferem aos auditores e organizações que as implementam, com métodos de deteção e métricas de classificação de vulnerabilidades. Algumas destas metodologias cobrem não apenas as componentes técnicas como também as componentes de processos, humanas e físicas (OSSTMM), enquanto outras focam-se exclusivamente na componente técnica (PTES).

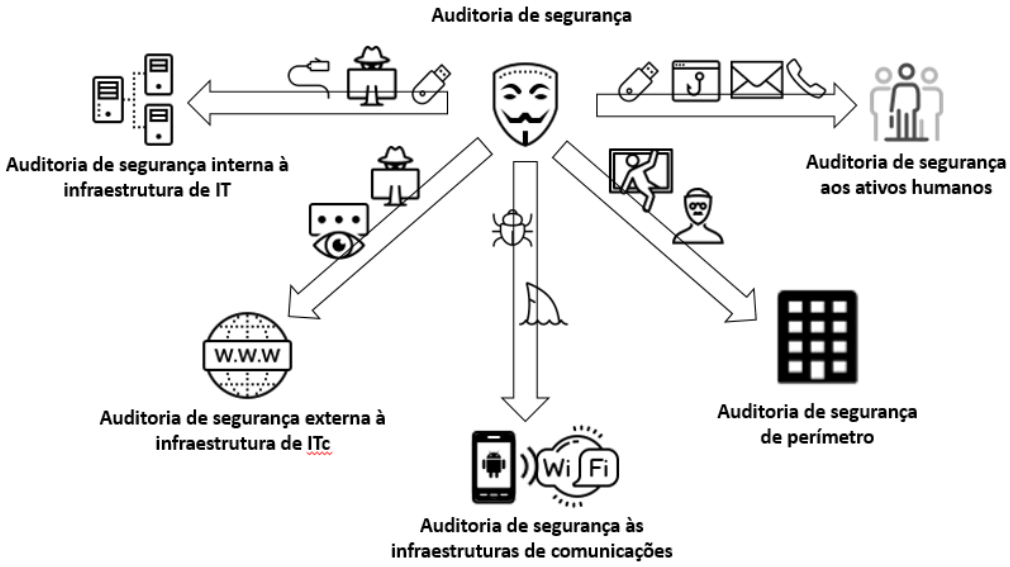


Figura 17 - Tipos de auditoria de segurança de informação

É importante salientar que existem duas formas de identificação de vulnerabilidades: um processo de Vulnerability Scan e um Pentesting. Um Vulnerability Scan (ou rastreamento de vulnerabilidades) tem como objetivo identificar vulnerabilidades sem as testar, pelo que este processo pode identificar falsos positivos. Contudo, os processos de rastreamento de vulnerabilidades dedicam maior parte do seu tempo a identificar a superfície de ataque. Um Pentesting tem como objetivo aferir a profundidade e a ameaça de uma vulnerabilidade, pelo que o seu principal objetivo é testar a robustez e a segurança de um sistema. Existem várias ferramentas que permitem o rastreio de vulnerabilidades, todas focadas para tecnologias

[47] https://www.isecom.org/OSSTMM.3.pdf

[48] https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf

[49] https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Web_Application_Penetration_Checklist_v1_1.pdf

[50] http://www.pentest-standard.org/index.php/Main_Page

específicas: Bases de Dados, Aplicações Web, WiFi, etc… dito isto, esta tese não enumera ferramentas específicas devido à extensa lista de possíveis vectores de ataque. No entanto, existem sistemas operativos tais como o Kali Linux ou o Parrot, que são *open source* e conferem aos utilizadores várias ferramentas de testes de segurança incluindo o rastreio de vulnerabilidades. Qualquer uma destas ferramentas é aplicável apenas no rastreio de vulnerabilidades (ou pentesting), mas são apenas aplicáveis a sistemas de informação. Com efeito, os métodos de identificação de vulnerabilidades em processos, passam obrigatoriamente por auditorias de testes de introdução (pentesting), nos quais deverão ser explorados vetores de ataque que testem o fator humano, como por exemplo: *emails* de *phishing*, uso de dispositivos amovíveis desconhecidos, telefonemas, entre outros…

O caracter periódico da identificação de vulnerabilidades justifica-se com o facto de que as redes e processos estão em constante evolução, pelo que cada *update*, novo *software ou novo* processo pode expor a organização a novos riscos. Contudo, devido ao seu carácter periódico, PMEs recorrem normalmente a serviços de auditoria externos para a execução da tarefa de dentificação de vulnerabilidades. Estes processos de identificação de vulnerabilidades são normalmente encomendados em formato de serviço de auditoria, mas por vezes já se encontram integrados nos serviços de controlo de qualidade das organizações.

5.5 Gestão de Acessos

Um dos principais objetivos de todas as normas de segurança existentes, é a capacitação das organizações em controlar os acessos aos seus ativos de informação, e em particular às redes e sistemas[51]. Mas com o aumento de plataformas informáticas e proliferação de aplicações de negócio e sistemas, a superfície de ataque aos sistemas de informação aumenta, pelo que o esforço de defender estes sistemas também aumenta, porque mais sistemas independentes significa mais possíveis pontos de acesso. Além disso, estes" acessos à informação" são frequentemente protegidos com palavras-passe, o que apesar de ser uma boa prática, obriga os utilizadores a decorarem e usarem palavras-passe diferentes para todos estes sistemas. Acresce ainda que o sistema de proteção de palavras passe, por si, não é suficiente para garantir a confidencialidade da informação (garantindo a autenticidade do acesso à mesma), porque entre outras razões, todas as palavras-passe perdem força como tempo52, pelo que as mesmas devem ser alteradas periodicamente. Ora, tal constitui um esforço adicional aos

[51] Este requisito é previsto não apenas no QNRCS (nomeadamente nos objetivos PR.GA-1, PR.GA-3, PR.GA-4, PR.GA-6 e PR.GA-7), mas também na RCM 41 / 2018 (na capacidade de autenticar utilizadores, de caráter obrigatório). De um ponto de vista mais holístico, a ISO 27001 também dá indicações relativamente ao controlo de acessos.

[52] Se por hipótese, piratas usarem técnicas de "brute force" ou recorrerem a *leaks* de credenciais existentes na Internet, então existe uma forte probabilidade de os mesmos terem acesso às credenciais dos sistemas de informação das organizações e dos particulares.

utilizadores que devem alterar as suas palavras-passe, e de cada sistema, regularmente; o que no limite poderá ser impraticável.

5.5.1 Sistemas de Gestão de Identidades e Acessos

Cada vez mais se recorre a soluções técnicas de sistemas de gestão de identidades e acessos, as quais em articulação com políticas de gestão de acesso e uso responsável conferem uma proteção bastante mais robusta aos sistemas e redes das organizações em matéria de autenticação e confidencialidade. Sistemas de gestão de identidades e acessos permitem às organizações centralizar os vários acessos dos seus sistemas de informação num único ponto de entrada, adicionando a possibilidade de criar diferentes "contas" de acesso com diferentes privilégios de acesso à informação, possibilitando assim o princípio da segmentação do acesso à informação, e por conseguinte, a possibilidade de garantir o princípio do "menor privilégio"[53]. Este método também assegura o princípio de "não repúdio"[54], pelo que só assim se conseguirá identificar o responsável pelo tratamento da informação.

Um sistema de gestão de acessos pode ser composto por vários componentes, entre os quais se destacam os seguintes:

- **Diretório LDAP**: este componente é o mais importante deste conjunto. É o diretório no qual são criadas as várias contas de utilizador que compõem a organização, através da criação de domínios. Esta diretoria pode conter desde dados pessoais de utilizadores até dados técnicos de outros ativos da organização (nem todos os ativos são pessoas), como computadores portáteis ou contas de utilizador para sistemas de automação. Este diretório contém também as credenciais dos utilizadores, pelo no papel de arquitetura de IT, é a componente que centralizará todos os logins da organização (aplicações, WiFi, etc…). Estes diretórios ligam-se às várias aplicações que servem através do protocolo LDAP. Existem várias soluções no mercado para diretórios LDAP, gratuitos ou pagos, dos quais se destacam o OpenLDAP (que configura uma solução open source) e o Active Directory da Microsoft (solução paga). Enquanto que as soluções *open source* permitem o uso gratuito deste serviço, a sua falta de suporte e por vezes difícil integração com as aplicações constituem uma desvantagem, que soluções como o *Active Directory* – embora pagas - não padecem.
- **Sistema RADIUS**: embora opcional e por vezes considerado exagerado para implementar em organizações de micro e pequena dimensão, este sistema garante que os utilizadores que acedem a uma rede sem fios beneficiam da mesma autenticação que beneficiam no seu sistema operativo, email ou outra aplicação de negócio. Na

[53] Princípio que insiste que um utilizador só deve ter acesso à informação estritamente necessária.

[54] O princípio de não repúdio visa garantir que um autor singular é identificado por executar uma ação.

perspetiva de arquitetura de rede, este sistema situa-se entre o ponto de acesso de rede e o diretório LDAP.

Existem outros sistemas considerados de "componentes do sistema de gestão de identidades e acessos" que poderão ser úteis configurar nas organizações (tais como servidor DHCP ou DNS), mas que em organizações de pequena ou micro dimensão poderão não se justificar na lógica de custo/ benefício.

Estes sistemas podem ser adquiridos separadamente; contudo existem soluções que já possuem todos estes componentes num único sistema. De facto, sistemas operativos como o Microsoft Server[55] ou Zentyal[56] (a homóloga Linux) conferem aos utilizadores todos estes componentes fundamentais para a implementação de gestão de controlo de acessos, o que constitui uma excelente simplificação quer da gestão de rede quer no próprio processo de implementação do sistema.

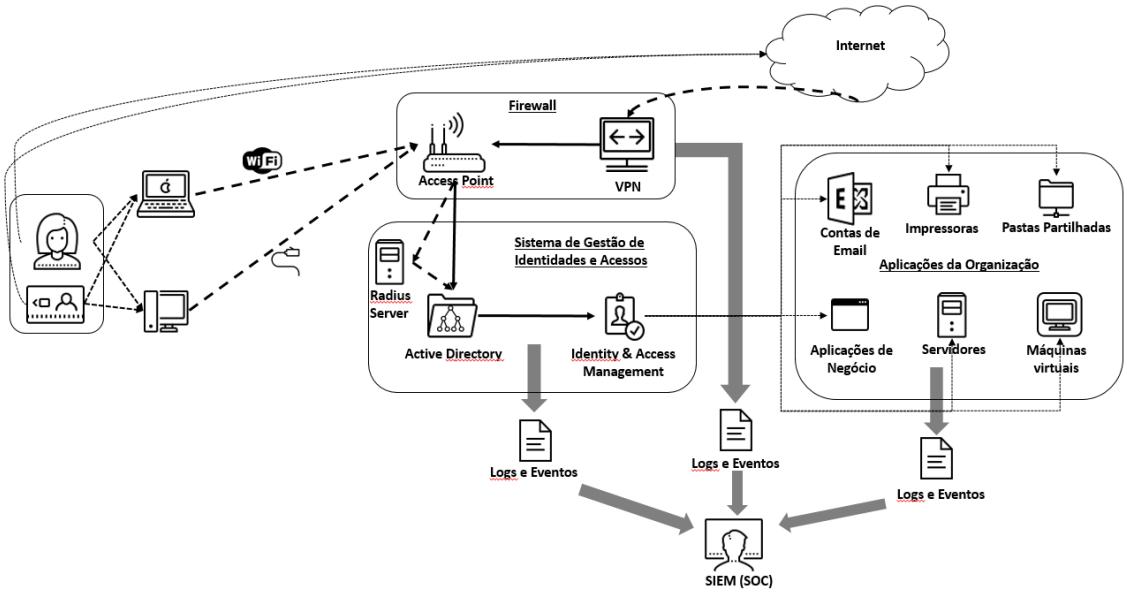


Figura 18 - Processo de Gestão de Acessos numa perspetiva de arquitetura de rede

5.5.2 Sistemas de Múltipla Autenticação

Com o objetivo de reforçar ainda mais a segurança da capacidade de autenticação das redes e sistemas de informação, o QNRCS recomenda a implementação de, pelo menos, mais um fator

[55] Microsoft Server 2016 e versões posteriores possui a funcionalidade de Microsoft Identity Manager bem como de Active Directory.

[56] ZenTyal é um servidor Linux Ubuntu com as mesmas capacidades de um Windows Server. A solução ZenTyal possui uma versão paga e uma versão "*Community*" gratuita.

de autenticação nestes sistemas[57]. Tipicamente os fatores de autenticação visam identificar o dono de uma conta através de:

1. Algo que o utilizador sabe, como por exemplo uma palavra-passe;
2. Algo que o utilizador possui, como um cartão ou outro objeto exclusivo deste utilizador;
3. Algo que o utilizador é, nomeadamente efetuando a identificação através de leituras biométricas.

Assim, é recomendado que no processo de implementação da autenticação por múltiplos fatores, o implementador utilize pelo menos 2 dos 3 métodos enumerados acima. Assim, objetivando o tipo de organizações que constituem a motivação desta tese, considera-se que se opte pelas soluções de mais fácil implementação e de menor custo. Neste sentido, será mais prudente optar-se por mecanismos de autenticação que façam uso de objetos que os utilizadores já possuam, como cartões de cidadão ou de telemóveis (através do uso de SMSs ou de aplicações de *tokens*). Contudo, a integração com sistemas de autenticação por *token* por aplicação ou SMS requer algum esforço de integração, pelo que a existência de leitores de cartões existentes em alguns computadores portáteis faz com que esta opção seja a mais apetecível de implementar.

5.5.3 Auditoria e controlo de acessos

Um requisito crítico para que estes sistemas de gestão de identidades e acessos funcionem, é que os mesmos sejam monitorizados[58]. Tal significa que estes sistemas deverão possibilitar aos seus operadores consultar em qualquer momento a informação por aqueles gerada, nomeadamente no que respeita aos acessos de contas de utilizador, a aplicações de negócio e outros sistemas. Felizmente todos estes sistemas geram registos de atividade (*logs* e eventos), pelo que os mesmos poderão ser consultados tanto no contexto proactivo como reativo de controlo de acessos.

No entanto, dado que estamos a lidar com vários sistemas em simultâneo (Diretoria LDAP, aplicações de negócio, etc…), o processo de gestão de identidades e acessos deverá ter em conta a consulta de registos de vários sistemas independentes e interligados, como ainda a sua correlação para efeitos de contextualização de eventos. Para tal, não é exequível que o operador efetue a consulta de sistema a sistema, pelo que fará sentido que o mesmo centralize os registos numa única plataforma, e que de lá efetue a sua monitorização. Assim, a monitorização de eventos de segurança relacionada com os acessos a redes e sistemas

[57] O mesmo requisito é também indicado com cariz obrigatório na RCM 41 / 2018 (nomeadamente na' Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações'.

[58] Requisitado no QNRCS e na RCM 41 / 2018 (na capacidade "Capacidade de monitorização, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis").

deverá ser garantida pelo sistema SIEM da organização, o qual merecerá o seu próprio capítulo nesta tese.

Outro requisito fundamental que se exige deste sistema de gestão de identidades e acessos, é a capacidade de se auditar[59]. Ou seja, que o mesmo tenha a capacidade de aferir se um utilizador tem produzido atividade num período de tempo, e se não, ter a capacidade de o desativar. Estas soluções tipicamente vêm capacitadas com esta funcionalidade. De facto, estes sistemas permitem automatizar estes processos bem como processos de validade de palavra-passe, impondo assim aos utilizadores a tarefa periódica de alteração de palavra-passe de acordo com a política estabelecida.

5.6 Plano de Continuidade de Negócio

O plano de continuidade de Negócio (PCN) é um processo crítico em qualquer organização, pois é o processo pelo qual se garante a reposição de serviço após um incidente. Este processo deve identificar junto dos processos de gestão de risco e gestão de incidentes os potenciais cenários de disrupção de serviço e planear uma resposta para cada cenário de forma a restabelecer o serviço no menor espaço de tempo possível, minimizando assim o impacto do incidente. Do ponto de vista organizacional, o PCN abrange toda a organização, pelo que os seus processos devem ser aprovados pela administração e comunicados não apenas aos colaboradores, como também a outras partes interessadas externas, tais como fornecedores, clientes ou outros. Aliás, o envolvimento da administração é chave quando os principais obstáculos do planeamento de continuidade de negócio se prendem com a falta de orçamento disponível para o efeito, como também a ausência de consciencialização dos colaboradores como um todo.

[59] Também previsto no QNRCS e na RCM 41 / 2018.

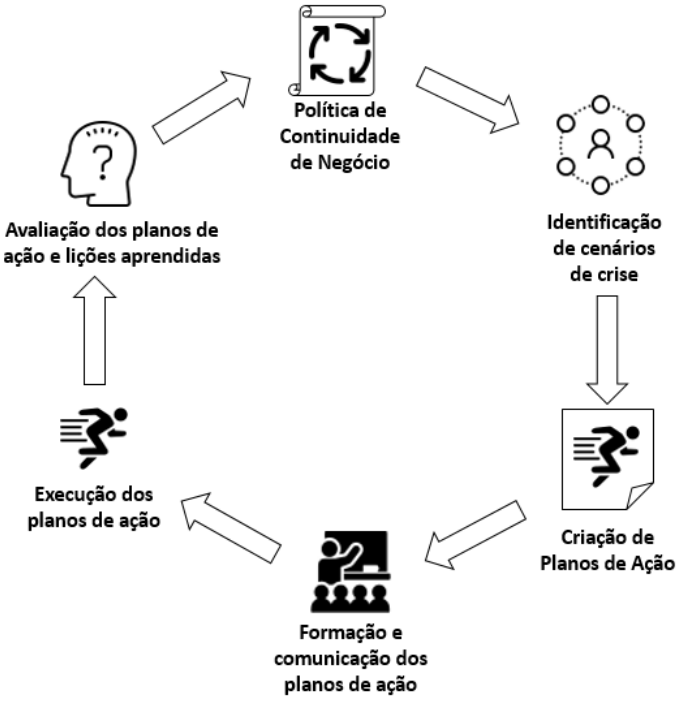


Figura 19 - Ciclo de vida da política de Continuidade de negócio

Entretanto, como já foi dito, o PCN deve ser alvo de revisão contínua, porque os meios técnicos evoluem com o tempo e as ameaças também. Assim, os planos de continuidade de negócio e recuperação de desastres devem-se readaptar às novas circunstâncias. Então, é imperativo que o PCN seja alvo de testes, não apenas para identificar possíveis lacunas e problemas no plano, mas também para implementar formações para que os colaboradores estejam devidamente preparados para executar os procedimentos do PCN quando necessário.

Figura 20 - *Use Case* de execução de um plano de ação

Existem vários guias que servem como linhas de orientação para a implementação de PCNs, nomeadamente as normas ISO 22301, ISO 27002 ou ISO 27031, pelo que esta tese não se alongará a descrever bases teóricas do PCN. No entanto, de uma maneira geral, o PCN deve contar com 4 categorias, cada uma orientada para uma etapa das ações de continuidade e com objetivos diferentes. Estas são:

- **Plano de Contingência ou Emergência:** utilizado em último caso, quanto todas as outras atividades preventivas tiverem falhado.
- **Plano de Recuperação de Desastres (Disaster Recovery)**: é o planeamento de ações para um momento pós-crise ou contingência. Assim, tem como objetivo o restabelecimento da operação da organização.

- **Plano de Gestão de Crises**: este plano define as responsabilidades de cada equipa e colaboradores envolvidos no processo do plano de contingência, ao longo de todo o período da crise (antes, durante e depois).
- **Plano de Continuidade Operacional:** O plano de continuidade operacional deve definir os SLAs (Service Level Agreements) dos períodos de resolução de incidentes, bem como os RPOs (Recovery Point Objectives) e os RTOs (Recovery Time Objectives) dos backups.

Todas estas definições devem ser oficializadas numa política de Plano de Continuidade de Negócio. Embora a política em si não deva ser partilhada com terceiros, algumas tarefas deverão ser, nomeadamente as que requerem participação de fornecedores e por vezes de clientes.

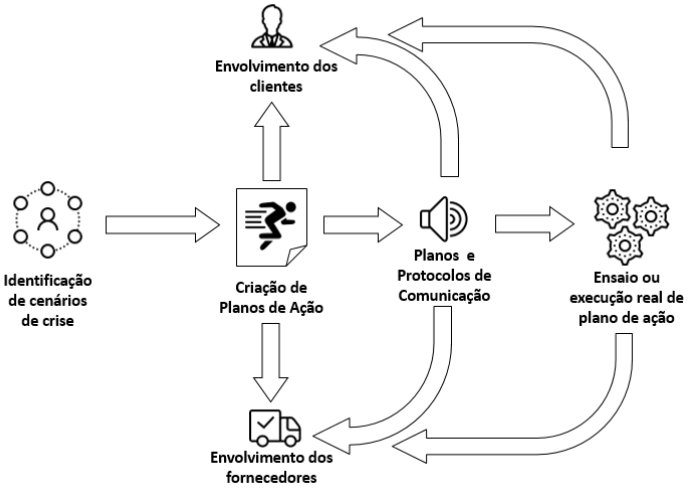


Figura 21 - Envolvimento de terceiros

5.7 Política de Backups

Backups são críticos para qualquer organização[60]. Este procedimento é muito importante para garantir a recuperação de sistemas após disrupção de serviço ou remoção indevida de ficheiros. Adicionalmente, muitas organizações são obrigadas a arquivar documentação durante certos prazos estipulados por lei61.

[60] Requisito do QNRCS (PR.PI-4), da RCM 41/2018 e da ISO 27001.

[61] Como faturas, dados pessoais e outros documentos.

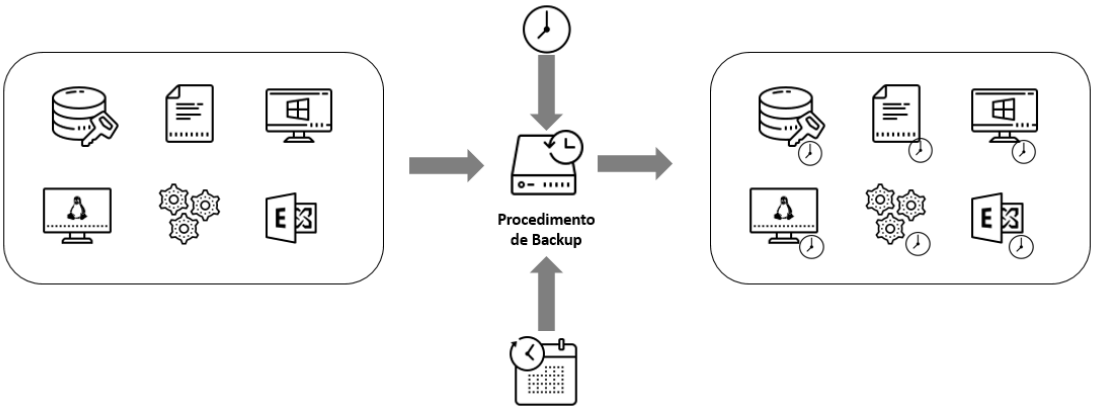


Figura 22- Processo de Backup

5.7.1 Conceitos

A estratégia de Backup tem como objetivo salvaguardar os dados que sejam críticos para o negócio da organização. Neste sentido, é fundamental copiar os dados relevantes da organização num período regular aceitável para uma localização segura, localização esta que deve assegurar a confidencialidade, disponibilidade e integridade dos dados.

Sempre que a tecnologia assim o permita, os processos de backup e restauro devem seguir as 4 linhas basilares da estratégia de backup, as quais são:

- **Automação**: a automação dos processos de backup e restauro, por via de meios técnicos e informáticos, minimiza a margem erro de tarefas repetitivas quando comparado com a execução do processo por um humano. Neste sentido, garante-se não apenas a regularidade do processo como também o registo da sua atividade.
- **Regulação**: a periodicidade e tipos de backup devem-se adequar à quantidade de informação produzida com a finalidade de minimizar a perda de dados em caso de disrupção de serviço, equacionando simultaneamente os meios de armazenamento disponíveis e os tempos de procedimento de backups.
- **Duplicação**: a redundância assegura a redução do risco de perda dos dados salvaguardados. Assim, os dados devem ser guardados localmente – *on-site* (redundância local: num sistema independente aos sistemas visados na política de backup) e remotamente – *off-site* (redundância geográfica: num local que não esteja exposto aos mesmos riscos de natureza ambiental, social e geográfica que o local *on-site*). Tendo em mente a redução do tempo de backup e reposição, os processos de backup deverão salvaguardar os seus dados para o local *on-site*, transformando o local *off-site* numa salvaguarda dos dados deste último.
- **Restauro**: os procedimentos de restauro deverão ser testados com frequência superior a duas vezes por ano. Os testes de restauro deverão abranger todos os sistemas cujos dados foram alvo de backup. Assim, todos os sistemas cujos dados são alvos de backup deverão ser objeto de teste do procedimento de restauro.

A política de backup deverá ser alvo de revisão periódica. Assim, de forma a aferir a sua eficácia, esta deverá produzir indicadores de performance - *KPIs*.
Aquando da elaboração desta política, a organização deverá ter em consideração os planos de Recuperação de Desastres e nomeadamente os conceitos de RTO e RPO. *Recovery Time Objective* (RTO) é o período máximo tolerável de tempo em que um computador, sistema, rede ou aplicação pode ficar inativa após uma falha ou desastre. *Recovery Point Objective* (POR) é a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações normais sejam retomadas se um computador, sistema ou rede ficar inativo como resultado de uma falha de hardware, programa ou comunicação. Estes dois conceitos são muito importantes para serem considerados no momento de projeção da política de backups.

5.8 SIEM

Um dos principais requisitos de QNRCS é a capacitação da organização de desenvolver práticas adequadas e atempadas à deteção da ocorrência de eventos de cibersegurança, por via da monitorização contínua das redes e sistemas de informação e da implementação de processos de deteção, a qual se reflete na capacidade "Identificar" anunciada pelo QNRCS. Todos os componentes e sistemas efetuam um registo da sua atividade, materializada na escrita de *logs* ou de eventos (no caso do Windows por exemplo). A monitorização constante da atividade das redes e sistemas é alcançada através da leitura em tempo real destes *logs* e eventos. Esta prática constitui uma das pedras basilares da cibersegurança já que é através da deteção de comportamentos anómalos dos sistemas e redes que se detetam ataques ou possíveis ataques ainda por se consumarem. No entanto, a constatação de comportamentos anormais num componente de sistema ou de rede poderá resultar em conclusões erradas, pelo que um comportamento anómalo poderá indicar um incidente "falso positivo" – sugerir que há um problema de segurança quando não há – ou um comportamento normal sugerir um incidente "falso negativo" – indicar que não existe nenhum problema de cibersegurança que de facto existe. É por isso que a monitorização de um componente de rede ou de sistema deve ser sempre contextualizada com o comportamento dos restantes componentes, pois é através da observação dos comportamentos de todos os componentes em simultâneo e de uma análise comportamental holística da rede e sistemas como um todo, que um utilizador consegue aferir com mais precisão se está diante de um incidente de segurança. Em virtude de os ataques informáticos serem cada vez mais sofisticados, também a sua deteção se torna mais difícil e complexa.

Todavia, a monitorização simultânea de vários sistemas e componentes de rede revela-se uma tarefa quase humanamente impossível, na medida que o operador ou operadores devem não apenas lidar com um fluxo de informação elevado e contínuo, como também devem

constantemente contextualizar o comportamento do sistema como um todo enquanto interpretam os dados que recebem, acrescendo ainda a constante atualização e estudo de novos ataques e dos seus comportamentos e sintomas. É por este motivo que é imperativo recorrer-se a um sistema de monitorização de eventos e incidentes (SIEM – Security Incident & Event Management). Um SIEM é uma ferramenta que permite endereçar de forma eficaz este desafio, na medida que permite, entre outras funcionalidades:

- Agregar e centralizar *logs* e eventos dos vários componentes de rede e sistemas numa única ferramenta;
- Configurar a deteção de padrões de comportamento que indiciem a possibilidade ou eminência de ataque;
- Alimentar automaticamente a ferramenta com novos padrões de comportamento de ataques através da ligação a serviços de Cyber Threat Intelligence;
- Deteção automática de comportamentos anormais através de inteligência artificial
- Configuração de alarmística personalizada de acordo com a gravidade do evento ou incidente (email, SMS, etc…);

Estas funcionalidades materializadas numa ferramenta SIEM, permitem às organizações não apenas cumprirem com os requisitos de deteção de incidentes de segurança como também servirem de facilitadores de conformidade com outros requisitos, tais como o controlo de acessos. Ou seja, mediante correta configuração, o operador do SIEM consegue controlar em tempo real quais os utilizadores que acedem a aplicações de negócio (no caso de acesso a aplicações) ou que utilizadores acedem a meios físicos (no caso de sistemas biométricos ligados em rede ao SIEM).

5.9 SOC

É relevante ainda dizer que a monitorização de redes e sistemas deve ser encarada como uma tarefa contínua 24x7, isto porque as ameaças não tiram fins-de-semana nem têm horário de expediente. É neste sentido que o QNRCS recomenda a criação de um SOC. De acordo com o documento, o SOC é um centro de operações de segurança, é tanto a equipa, que frequentemente opera em turnos de 24h/7 dias da semana, como as instalações dedicadas e organizadas para prevenir, detetar, avaliar e responder a ameaças e incidentes de cibersegurança, e para avaliar e cumprir com a conformidade das leis locais em vigor. Ou seja, no caso de uma organização de pequena ou micro dimensão, este papel é assumido pelo operador do SIEM, pelo que o SIEM é a principal ferramenta de qualquer SOC. Tal sugere que a organização adote um modelo adequado a esta necessidade, o qual pode passar pela atribuição de turnos entre operadores do SIEM, ou pela adoção de um modelo 8x5 acompanhado com alarmística para as restantes horas, ou ainda através de um modelo de outsourcing parcial ou total desta tarefa. De facto, o QNRCS sugere alguns modelos de funcionamento do SOC:

Tipo de SOC	Instalações	Equipas	Operação	Atividade	Outros Serviços
Virtual	Sem instalações dedicadas	Equipa com alocação parcial e sem exclusividade	Operação 9x5 com resposta no próximo dia útil	reativo, apenas despoletando quando aparece um alerta crítico ou incidente	
Dedicado	Instalações dedicadas	Equipa interna com alocação total e em exclusividade	Operação 24x7	reativo e pró-ativo	
Distribuído	Instalações dedicadas	Equipas internas com alocação total ou parcial	Operação 24x7 ou 9x5, dependendo do local físico	reativo e pró-ativo	Possibilidade de partilha de responsabilidades com parceiros especializados em cibersegurança.
De Comando	Instalações dedicadas	Equipas internas com alocação total	Operação 9x5	reativo e pró-ativo	Providencia inteligência sobre ameaças e visão situacional global.
Multifunções	Instalações dedicadas	Equipas internas com alocação total;	Operação 24x7;	reativo e pró-ativo	Providencia, também, serviços de operação e manutenção de redes ou sistemas de informação.
De Fusão	Instalações dedicadas;	Equipas internas com alocação total;	Operação 24x7;	Reativo e pró-ativo;	Integra as equipas de resposta a incidentes (CSIRT) ou de operação dos equipamentos de segurança e rede.
Externalizado	Sem instalações dedicadas	Equipas externas com alocação total	Operação 24x7	reativo e pró-ativo	Supervisão das atividades por alguém interno à

					organização.

Tabela 19 - Tipos de SOC [1]

Ainda dentro do âmbito da deteção e resposta de incidentes, o QNRCS sugere ainda a criação de um CSIRT. Uma equipa de CSIRT é uma equipa de peritos de segurança informática que tem como principal atividade responder aos incidentes. Presta os serviços necessários para os gerir e ajudar os seus utilizadores a recuperarem das violações da segurança que ocorram. Ora, no caso de uma organização pequena, cuja infraestrutura de sistemas de informação é proporcional à sua dimensão, é esperado que o operador do SIEM reúna na sua pessoa as funcionalidades de SOC e CSIRT.

Atendendo à realidade das pequenas e microempresas, é expectável que se as mesmas optarem por implementar estas medidas, optem pela criação de um SOC no modelo Virtual, distribuído ou externalizado, ou até um modelo hibrido entre os 3. Em todo o caso, a organização deve definir os procedimentos de resposta, mitigação e comunicação em caso de incidente de segurança com as partes interessadas. Todos estes procedimentos deverão ser do conhecimento dos colaboradores envolvidos (o que no caso de uma microempresa deverão ser todos). No caso de estudo em análise, recomenda-se à organização que adote um modelo de SOC Virtual numa primeira fase, podendo posteriormente expandir para um modelo SOC Distribuído.

Em qualquer caso, a tarefa de monitorização de eventos e incidentes de segurança revela-se um esforço que muito provavelmente obrigará à contratação de uma pessoa dedicada. Em micro e pequenas empresas, a contratação de uma pessoa dedicada à gestão dos temas de segurança (incluindo a do SOC) pode constituir um encargo elevado – se por exemplo uma empresa de 10 pessoas necessitar de contratar uma pessoa para desempenhar as funções de segurança referidas no QNRCS, tal constitui um aumento de 10% do pessoal, acrescendo ainda que esta pessoa deverá ter conhecimentos técnicos de informática e segurança (o que provavelmente encarecerá o custo da contratação). É por este motivo que muitas empresas optam por externalizar parte ou a totalidade da sua gestão de IT, e por arrasto as funções de segurança informática.

Independentemente do modelo de SOC a adotar, se a organização possuir uma infraestrutura de IT própria (em detrimento de ter os seus ativos em *cloud*), então deverá também integrar o SIEM na sua infraestrutura, podendo posteriormente o operador interno aceder diretamente à ferramenta ou através de VPN se for um operador externo.

Existem várias soluções de SIEM disponíveis no mercado, algumas pagas e outras com modalidades gratuitas. E usual algumas soluções SIEM terem versões pagas e versões gratuitas com menos funcionalidades. Porém, dada a baixa complexidade média dos sistemas e infraestruturas de IT das micro e pequenas empresas, as funcionalidades básicas (gratuitas) destes SIEMs vão ao encontro das necessidades destas organizações. Alguns exemplos destas ferramentas são:

- **SPLUNK Free**: Splunk é um dos SIEMs mais conhecidos e usados no mercado. Splunk Free, como o próprio nome sugere, é a versão gratuita do Splunk. Este SIEM gratuito permite indexar até 500 MB por dia e não expira, pelo que 500 MB diários é normalmente suficiente para organizações de pequena ou micro dimensão. Contudo, se a organização necessitar de mais tráfego diário, poderá sempre expandir a sua licença para a versão Enterprise (paga). O Splunk Enterprise confere visibilidade em tempo real, permitindo automatizar a coleta de logs, indexação e alerta de dados. O Splunk Enterprise é um programa abrangente do SIEM. Embora o Splunk Free compartilhe muitos de seus recursos, este possui algumas limitações face à versão Enterprise.
- **Graylog**: Graylog é uma solução de gestão de *logs* centralizado *open source* para recolha, armazenamento e análise em tempo real. Graylog é totalmente *multi-tenant*, inclui Elasticsearch *multi-threaded*, Mongo DB e é facilmente integrado com outros componentes em sua pilha de tecnologia - até mesmo outras soluções de gestão de *logs*.

Existem mais ferramentas, sendo que estas são apenas exemplos. Estas podem ser instaladas "on premesis" na própria infraestrutura da organização numa máquina virtual dedicada. Apesar de maior parte das vezes a sua instalação ser relativamente fácil, a sua configuração poder-se-á revelar algo trabalhosa.

5.10 Plano de Formações e Comunicações Internas

Que mecanismo garante que a correta articulação de atividades entre as diversas partes interessadas num processo de segurança ou de negócio? Este mecanismo é a comunicação.

5.10.1 Plano de Comunicações

O plano de comunicações deve considerar os diferentes cenários previstos no plano de Gestão de Incidentes, Gestão de Alterações e Continuidade de Negócio, bem como as próprias políticas de segurança da organização que deverão ser comunicadas com todas as partes interessadas (colaboradores, clientes, fornecedores e o público).

	Colaboradores	Clientes	Fornecedores	
Políticas e Procedimentos	Notificações e-mail e formações presenciais ou e-learning	Notificações e-mail	Notificações e-mail	Página da Organização
Formações	Notificações e-mail e formações presenciais ou e-learning		Notificações e-mail e formações presenciais ou e-learning	
Gestão de Incidentes e Alterações	Consoante a criticidade, por notificação e-mail, telefone ou presencial	Consoante a criticidade, por notificação e-mail, telefone ou presencial	Consoante a criticidade, por notificação e-mail ou telefone	

Tabela 20 - Exemplo de plano de comunicação

A formação também deverá ser considerada uma componente da comunicação, sendo mais exaustiva do que a última. Os meios de comunicação deverão ser ajustados à criticidade da situação, conforme mostra a figura acima. Note-se que a título de controlo, este plano deve ser auditável, pelo que o plano de comunicações deverá sempre contemplar a criação de registos de atividade. Ou seja, todas as formações deverão ser assinadas pelos formadores e formandos.

5.11 Formação e sensibilização

O elo mais fraco na cadeia de segurança de informação é o Humano. Por este motivo, é imperativo garantir que este elo se torne tanto mais robusto quanto possível. De facto, todos os mecanismos automáticos de segurança de nada valem se o fator humano, que é o principal na segurança de informação falhar. Processos são assegurados por humanos, que os executam ou desencadeiam. Mas o que assegura que os seres humanos executam corretamente e de forma segura as suas tarefas?

O QNRCS não dá suficiente enfase a este tema, pelo que esta tese se propõe sugerir algumas orientações, uma vez que a formação e sensibilização de temas de segurança de informação são talvez o processo mais importante da segurança de informação numa organização. As formações / ações de sensibilização podem ser presenciais ou remotas (online). No entanto, a melhor solução passará por uma solução híbrida – presencial numa primeira fase e digital subsequentemente. É importante, no entanto garantir que os utilizadores retiveram a

informação transmitida, pelo que as ações de formação / sensibilização devem ser acompanhadas por testes e/ou testes de penetração para garantir a resiliência humana contra ameaças de cibersegurança.

A atividade da sensibilização é usualmente externalizada, ou seja, muitas organizações optam por comprar serviços de formação e sensibilização de segurança de informação. No entanto, pode existir a necessidade da qualquer organização implementar o seu próprio processo de formação e sensibilização, em virtude de especificidades do seu negócio. Para os casos em que a organização implementa o seu próprio processo de formação / sensibilização, é importante que a mesma defina os seus conteúdos e que os disponibilize para serem consultados sempre que a situação assim o exigir.

5.11.1 Ferramentas digitais

Em fases de maturidade mais iniciais, as organizações podem recorrer a conteúdos online, tais como os que são disponibilizados pelo CNCS. Avisos de novas formações podem ser enviados através do email, e conteúdos feitos criados em Power-Point ou retiradas da internet (ex: CNCS). Alternativamente, pode-se recorrer a conteúdos pagos de baixo custo de cibersegurança, tais como o Udemy ou Cybrary. No entanto, pode haver o interesse de a organização constituir a sua própria ferramenta de formação e sensibilização, na qual a organização possui uma gestão dos conteúdos por utilizador, e que na qual, também pode usar para divulgar outros conteúdos relevantes à segurança de informação (ex: políticas de segurança).

Para o efeito, efetuou-se uma pesquisa de ferramentas que satisfaçam esta necessidade, designadamente ferramentas de LMS (*Learning Management System*). Dada a dimensão da organização em análise, optou-se por pesquisar por ferramentas LMS gratuitas ou *open-source*. Pequenas empresas que usam aplicações LMS gratuitas têm custos mais baixos, mas não beneficiam de todas as funcionalidades disponíveis, pelo que terão de pagar para ter acesso a estas últimas. Porém, é de salientar que muitas das funcionalidades disponíveis nas versões gratuitas cobrem amplamente as necessidades das PMEs.

Para além das ferramentas gratuitas, existe outro tipo de ferramentas *open-source*, que permitem mais personalização sem necessitar de comprar licenças. Algumas soluções funcionam em modo "*on-premesis*", outras permitem funcionar em *cloud*, poupando a empresa de investir em infraestrutura, e noutros casos ambas as hipóteses estão disponíveis. Uma ferramenta LMS proporciona a vantagem de automatizar e registar processos de formação, o que confere à organização uma agilização destes processos como evidências destes para efeitos de auditoria. Das ferramentas pesquisadas, destacam-se as seguintes:

- **Forma LMS**[62]: o Forma LMS é uma ferramenta *open source* que permite gestão de *eLearning*, gestão de cursos, videoconferência, certificação, etc. Outros recursos incluem ferramentas de edição para gestão de utilizadores e função de geração de relatórios contendo dados sobre a participação dos formandos em cursos, conclusões, tarefas, etc. Além disso, o Forma LMS permite organizar cursos com base em categorias.
- **Moodle**[63]: o Moodle é uma plataforma gratuita *open source* que permite aos utilizadores criar cursos personalizados. Oferece ferramentas para gerir salas de aula virtuais, gerar certificados e medir o sucesso de programas de formação por meio de análises.

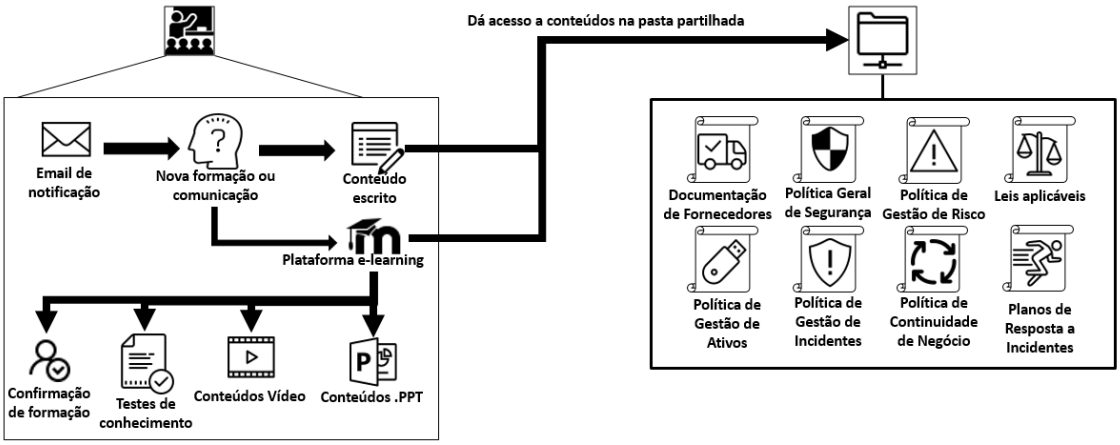


Figura 23 - Processo de formação contínua

5.11.2 Conteúdos

Com a proliferação de novos sistemas de informação e dispositivos, é crucial endereçar temas de S.I. que sejam os mais abrangentes possíveis. Assim fará sentido dividir os conteúdos de S.I. em duas categorias:

- **Conteúdos individuais**: boas práticas aplicáveis a qualquer indivíduo dentro ou fora do contexto da organização.
- **Conteúdos organizacionais**: boas práticas de cibersegurança aplicáveis no contexto organizacional.

As listas que se seguem são sugestões de temas para formação e sensibilização da segurança de informação [21].

[62] https://www.formalms.org/

[63] https://moodle.org/?lang=pt

5.11.2.1 Conteúdos individuais:

- **Navegação na Internet**: a correta navegação na Internet pode evitar muitas dores de cabeça à organização, pois a mesma constitui um vetor de ataque muito comum. Entre os tópicos abordados neste tema, devem-se considerar a correta utilização da Internet (utilização responsável e legal); a correta utilização dos sistemas de compras-online; correta utilização de downloads e as boas práticas de teletrabalho (incluindo boas práticas de vídeo conferência).
- **Manuseamento de contas de utilizador**: as quantidades de serviços online obrigam os utilizadores a possuírem várias contas para os diferentes serviços. Este facto faz com que a gestão de credenciais e ciclo de vida destas contas constitua uma tarefa pesada para os utilizadores, que por sua vez tendem a adotar posturas mais flexíveis e simplificadas à gestão de contas, o que compromete a sua segurança. Neste sentido, devem-se considerar tópicos de limitação de dados pessoais nas contas, configurações de passwords (gestão de passwords); uso de MFA[64] quando possível entre outros.
- **Manuseamento de dados e privacidade**: a segurança de informação de dados é responsabilidade de todos, não apenas da equipa de TI. Com efeito, é responsabilidade do utilizador salvaguardar a Confidencialidade, Integridade e Disponibilidade dos seus dados, pelo que é importante ter em mente os seguintes tópicos quando se abordar este tema: *backups*; encriptação e limitação de dados pessoais na web.
- **Utilização de email**: talvez a ferramenta mais utilizada pelas PMEs, este tema merece ser tratado à parte dos restantes. A má utilização desta ferramenta pode constituir uma vulnerabilidade que usualmente serve como principal vetor de ataque às PMEs. Dentro deste tema, devem-se considerar os seguintes tópicos: proteção contra-ataques de *phishing*; boas práticas de emails (correto reencaminhamento, scan de anexos, etc.); proteção contra emails de spam e uso correto de *webmails*.
- **Utilização de dispositivos móveis**: cada vez mais, a integração de dispositivos móveis se encontra mais integrada nas redes e sistemas de informação das organizações, pelo que a sua segurança não deve ser descurada. Assim, fará sentido considerar a sensibilização de tópicos como esquemas de fraude via telefone, a correta utilização de *QR codes*; boas práticas de segurança (encriptação de disco, evitar deixar os dispositivos no porta-bagagens do carro, *etc*); proteção contra *malware* em *smartphones*; correta utilização de aplicações de *smartphone*; entre outros.
- **Utilização de redes sociais**: muitos negócios dependem da utilização de redes sociais (publicidade de produtos, recrutamento, comunicação, *etc*), pelo que a correta utilização de redes sociais deve ser entendida como um processo da mais extrema importância. Neste tópico, será relevante abordar temas como o uso seguro das redes

[64] Multi Factor Authentication

sociais contra ataques de engenharia social, conteúdos maliciosos ou roubos de identidade; mas também o correto uso de aplicações de *messaging*[65] ou *blogs*.

- **Utilização de computadores pessoais**: talvez a principal suporte físico de trabalho das PMEs, a necessidade de medidas de segurança para este dispositivo é crítica. Como tal, devem ser considerados tópicos relativos à sua utilização, soluções *anti-malware*, *firewalls*, atualizações de sistema operativo entre outros.

5.11.2.2 Conteúdos organizacionais:

- **Controlo de acessos**: um dos principais objetivos de todas as normas de segurança existentes, é a capacitação das organizações em controlar os acessos aos seus ativos de informação, e em particular em redes e sistemas[66]. Neste sentido, será de considerar a abordagem aos tópicos de métodos de autenticação; controlo criptográfico, gestão de identidades e SSO[67].
- **Segurança aplicacional**: muitas PMEs possuem aplicações de negócio próprias, as quais constituem ativos críticos para as organizações. Assim, dever-se-ão considerar formações e sensibilizações neste tema, nomeadamente boas práticas de securização de aplicações web (gestão do seu ciclo de vida, gestão de vulnerabilidades, entre outros); desenvolvimento seguro; gestão de *patches*, uso de VPN entre outras medidas.
- **Planos de Continuidade de Negócio**: O plano de continuidade de Negócio (PCN) é um processo crítico em qualquer organização, pois é o processo pelo qual se garante a reposição de serviço após um incidente. Será de extrema importância garantir que todos os intervenientes saibam como agir na eventualidade de ativação de planos de contingência.
- **Privacidade de Dados e RGPD**: a entrada em vigor do RGPD a 28 de Maio de 2018 introduziu algumas obrigatoriedades aos processos da organização, que se a mesma não cumprir pode ser alvo de coima. Neste sentido, a organização (e por arrasto, os seus colaboradores) devem ter conhecimento dos requisitos da norma, bem como outras normas e decretos associados (ex: RCM 46/2018[68]).
- **Segurança de Email**: á parte das boas práticas de segurança de email já mencionadas, falta ainda mencionar as boas práticas de securização de email, as quais devem ser tidas em conta pela equipa de TI, como por exemplo: uso de certificados, assinaturas digitais, monitorização de emails de *phishing*, técnicas de gestão de *spam* entre outras.

---

[65] Tais como Whatsapp, Telegram ou Signal.

[66] Este requisito é previsto não apenas no QNRCS (nomeadamente nos objetivos PR.GA-1, PR.GA-3, PR.GA-4, PR.GA-6 e PR.GA-7), mas também na RCM 41 / 2018 (na capacidade de autenticar utilizadores, de caráter obrigatório). De um ponto de vista mais holístico, a ISO 27001 também dá indicações relativamente ao controlo de acessos.

[67] Single Sign-On

[68] Resolução de Conselho de Ministros d46 de 2018

- **Segurança dos RH**: já se mencionou que o elemento humano é o elo mais fraco, mas também o elo mais forte quando preparado. A garantia de que os utilizadores são alvo de ações de sensibilização é usualmente atribuída à equipa de RH.
- **Gestão de Segurança de TI e políticas de Segurança**: a gestão de TI é crítica para uma boa gestão da cibersegurança. Neste sentido é essencial garantir que a consciencialização da manutenção de processos críticos para a S.I., tais como a implementação da *frameworks* de cibersegurança e S.I.; gestão de ativos e gestão de risco.
- **Segurança de Redes**: se a segurança de informação no fator humano é o coração da cibersegurança, a segurança de redes é o seu cérbero, pelo que a importância de implementação não pode ser desvalorizada. Neste sentido, é necessário consciencializar os colaboradores para as boas práticas de utilização de redes wireless, DNS, IPV6; utilização de *software open source*; entre outros.
- **Segurança Física**: a cibersegurança também passa pela segurança física, razão pela qual as boas práticas da segurança física não podem ser negligenciadas (ex: a não partilha de credenciais ou cartões de acesso, uso de cadeados, etc).

5.11.3 Destinatários

A formação e sensibilização de segurança de informação deve ser orientada ao utilizador de acordo com a sua função, e, por conseguinte, com a sua exposição ao risco. A sobrecarga de informação (de formação / sensibilização) poderá ter um efeito adverso no utilizador, levando este último a menosprezar a informação adquirida. Deste modo, dividimos os utilizadores em 5 categorias, para melhor orientar os temas indicados acima às suas funções:

- **Administração**: pessoas com conhecimento estratégico da organização, usualmente são detentores de informação crítica, pelo que a sua segurança deve ser acautelada.
- **Financeiro**: esta categoria é usualmente alvo de ataques informáticos, tendo em conta que uma significativa fatia da motivação dos ataques informáticos é financeira e esta categoria tem acesso aos fundos das organizações.
- **Equipa de TI**: com responsabilidade de implementação das medidas técnicas, eles mesmos têm acesso a todos os sistemas de segurança de informação da organização.
- **Recursos Humanos**: a equipa de RH tem a responsabilidade de gerir temas relacionados com os colaboradores, e uma vez que normalmente têm acesso a todos os colaboradores, torna-se um alvo apetecível de ciberataques.
- **Geral**: todos os restantes operacionais da organização que não se enquadram nas categorias acima. Este grupo é vasto, pois pode albergar vários tipos de funções, desde administrativos até programadores.

5.11.4 Aplicabilidade

A relação entre a sensibilização dos temas abordados acima e o tipo de destinatário é representada na tabela seguinte.

Temas	Administração	Financeiro	Equipa de TI	RH	Geral
Navegação na Internet	Aplicável	Aplicável	Aplicável	Aplicável	Aplicável
Manuseamento de contas de utilizador	Aplicável	Aplicável	Aplicável	Aplicável	Aplicável
Manuseamento de dados e privacidade	N/A	Aplicável	Aplicável	Aplicável	Aplicável
Utilização de email	Aplicável	Aplicável	Aplicável	Aplicável	Aplicável
Utilização de dispositivos móveis	Aplicável	Aplicável	Aplicável	Aplicável	Aplicável
Utilização de redes sociais	N/A	N/A	N/A	Aplicável	N/A
Utilização de computadores pessoais	Aplicável	Aplicável	Aplicável	Aplicável	Aplicável
Controlo de acessos	N/A	N/A	Aplicável	N/A	N/A
Segurança aplicacional	N/A	N/A	Aplicável	N/A	N/A
Planos de Continuidade de Negócio	N/A	N/A	Aplicável	N/A	Aplicável
Privacidade de Dados e RGPD	Aplicável	N/A	Aplicável	Aplicável	N/A
Segurança de Email	N/A	N/A	Aplicável	N/A	N/A
Segurança de RH	N/A	N/A	N/A	Aplicável	N/A
Gestão de Segurança de TI e políticas de Segurança	Aplicável	N/A	Aplicável	N/A	N/A
Segurança de Redes	N/A	N/A	Aplicável	N/A	N/A
Segurança Física	Aplicável	Aplicável	Aplicável	Aplicável	Aplicável

Tabela 21 - Aplicabilidade de emas de security awareness por tipo de destinatário

5.12 Reporte de incidentes

Tal como todos os processos de segurança, os incidentes deverão ser reportados usando canais próprios pré-definidos e deverão ser criados registos da ocorrência. Tal deve acontecer para que o processo possa ser auditado e, por conseguinte, melhorado.

Várias organizações reportam incidentes usando o e-mail, porque permite não apenas manter um registo dos incidentes, como também é um meio de comunicação acessível às organizações. Outras organizações de maior dimensão, usam ferramentas próprias de reporte de Incidentes, tais como o EasyVista[69] ou ServiceDesk Plus da ManagaEngine[70], que associam incidentes a ativos e a resolução de problemas e gestão de risco. Estas soluções são licenciadas, mas permitem agregar vários processos numa única ferramenta, facilitando a gestão de todos estes processos.

No entanto, opções gratuitas como Mint ServiceDesk[71] permitem combinar gestão de ativos com gestão de Incidentes, pelo que não dispondo das mesmas capacidades que as soluções mencionadas acima, poderão revelar-se uma alternativa para micro e pequenas organizações. É preciso ter em conta que esta solução é ideal se se prever um crescimento da organização, caso contrário, uma pequena organização poderá utilizar um ficheiro ou até mesmo o email de

[69] https://www.easyvista.com/
[70] https://www.manageengine.com/products/service-desk/
[71] https://www.mintsd.com/

forma a registar os incidentes. Alternativamente, um SIEM também permite abertura de incidentes (na própria ferramenta como veremos no capítulo seguinte), mas normalmente estes incidentes restringem-se à dimensão dos incidentes por si detetados (ou seja, não inclui incidentes de ordem não digital – ex: violação de acesso físico).

5.12.1 Tipos de Notificação

Entretanto, à data da escrita do presente texto, foi dado a conhecer ao público um decreto lei (Decreto-lei 65/2021) que, entre outras medidas, dita regras quanto à forma como as organizações devem reportar os incidentes ao CNCS, nomeadamente: "

1 - *Por cada incidente que deva ser objeto de notificação ao abrigo do disposto no artigo anterior, as entidades devem submeter ao CNCS:*

a) Uma notificação inicial, nos termos do artigo seguinte;
b) Uma notificação de fim de impacto relevante ou substancial, nos termos do artigo 14.º;
c) Uma notificação final, nos termos do artigo 15.º

2 - Nos casos em que o incidente seja resolvido de forma imediata, nas primeiras duas horas após a sua deteção, as entidades podem enviar diretamente a notificação final com todos os campos de informação devidamente preenchidos, ficando dispensadas do envio das restantes notificações.[72]*"* sendo que **a notificação inicial** deve incluir:

a) "a) Nome, número de telefone e endereço de correio eletrónico de um representante da entidade, quando diferente do ponto de contacto permanente a que se refere o artigo 4.º, para efeito de um eventual contacto por parte do CNCS;
b) Data e hora do início ou, em caso de impossibilidade de o determinar, da deteção do incidente;
c) Breve descrição do incidente, incluindo a indicação da categoria da causa raiz e dos efeitos produzidos, de acordo com a taxonomia definida no artigo 16.º e, sempre que possível, o respetivo detalhe;
d) Estimativa possível do impacto, considerando:
    a. Número de utilizadores afetados pela perturbação do serviço;
    b. Duração do incidente;
    c. Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
e) Outra informação que a entidade considere relevante."

Também existem regras para notificações de fim de impacto relevante ou substancial:

[72] Artigo 12 do decreto-lei 65/2021

1 - A notificação de fim de impacto relevante ou substancial do incidente deve ser submetida ao CNCS logo que possível, dentro do prazo máximo de duas horas após a perda de impacto relevante ou substancial.

2 - A notificação de fim de impacto relevante ou substancial deve incluir a seguinte informação

a) Atualização da informação transmitida na notificação inicial, caso exista;
b) Breve descrição das medidas adotadas para a resolução do incidente;
c) Descrição da situação do impacto existente no momento da perda de impacto relevante ou substancial, nomeadamente:
    i. Número de utilizadores afetados pela perturbação do serviço;
    ii. Duração do incidente;
    iii. Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
    iv. Tempo estimado para a recuperação total dos serviços

Finalmente, a notificação final requer os seguintes procedimentos:

1 - A notificação final deve ser enviada no prazo de 30 dias úteis a contar do momento em que o incidente deixou de se verificar.

2 - A notificação final deve incluir a seguinte informação:

a) Data e hora em que o incidente assumiu o impacto relevante ou substancial;
b) Data e hora em que o incidente perdeu o impacto relevante ou substancial;
c) Impacto do incidente, considerando:
    i. Número de utilizadores afetados pela perturbação do serviço;
    ii. Duração do incidente;
    iii. Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
    iv. Descrição do incidente, com indicação da categoria da causa raiz e dos efeitos produzidos, de acordo com a taxonomia definida no artigo seguinte, e o respetivo detalhe;
d) Indicação das medidas adotadas para mitigar o incidente;
e) Descrição da situação residual do impacto existente à data da notificação final, nomeadamente:
    i. Número de utilizadores afetados pela perturbação do serviço;
    ii. Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
    iii. Tempo estimado para a recuperação total dos serviços ainda afetados;
f) Indicação, sempre que aplicável, da apresentação de notificação do incidente em causa às autoridades competentes, nomeadamente ao Ministério Público, à ANEPC, à

ANACOM, à CNPD e a outras autoridades setoriais, nos termos previstos nas disposições legais e regulamentares aplicáveis;

g) Outra informação que a entidade considere relevante.

Capítulo 6 – Conclusões

O QNRCS revela-se uma excelente iniciativa do Estado português em estabelecer padrões de segurança informática no tecido empresarial português (incluindo o setor público). De um ponto de vista de soberania nacional, é importante que os estados garantam a capacidade de defender os seus cidadãos[73] e o seu território. Mas o que acontece quando o território deixa de ser material e passa para o plano do abstrato? Sendo o Ciberespaço a materialização deste novo conceito de território abstrato, cabe ao Estado português tomar as medidas mais adequadas para proteger o "seu ciberespaço", e em última instância, o dos seus cidadãos. Esta proteção não se impõe apenas contra agentes externos, mas também se impõe contra agentes internos. E é neste contexto que nasceu o QNRCS. Apesar do QNRCS não se assumir como "uma norma de cibersegurança, mas sim como uma referência que permita identificar as normas, padrões e boas práticas existentes em vários domínios da segurança da informação", a verdade é que a sua implementação é cada vez mais relevante nos dias atuais, e a sua certificação cada vez mais provável[74].

Mas o decreto-lei que refere a possível certificação, reitera a sua aplicabilidade à Administração Pública, operadores de infraestruturas críticas e operadores de serviços essenciais, sendo que à data da escrita deste documento ainda não existe uma definição clara destes últimos. Assim, na ausência de critérios de conformidade e cumprimento do QNRCS, poder-se-á colocar a pergunta: tem que se cumprir com todas as subcategorias do QNRCS? Se sim, com que grau de maturidade?

Ao colocar a hipótese do pior cenário (todas as subcategorias com o grau de maturidade máximo), rapidamente se conclui que o QNRCS constituiria um peso demasiado elevado para as PMEs nacionais suportarem, devido aos custos da sua implementação, impedindo desta forma qualquer organização de dimensão mais pequena a fornecer serviços essenciais à sociedade. Assim, a presente tese propôs-se a:

1. Testar a abordagem[75] do QNRCS numa PME,
2. Estabelecer critérios de conformidade com QNRCS, e
3. Testar a adequação dos graus de maturidade do Quadro de Avaliação [2]

para que se pudesse aferir de que forma o QNRCS se pode adaptar às organizações mais pequenas, e desta forma ser mais inclusivo e abrangente para o tecido empresarial português.

[73] Como refere o constitucionalista Jorge Miranda, "O Estado promove a integração, a direção e a defesa da sociedade e, por arrastamento, a própria sobrevivência como um fim em si; […]".
[74] Á data da escrita deste texto, não existe nenhum critério de conformidade ou certificação, mas o Decreto-lei 65/2021 Artigo 1, 1b) prevê a sua certificação.
[75] Abordagem dos 7 passos, descritos no Quadro de Avaliação.

6.1. Observações na implementação do QNRCS numa PME

O QNRCS refere que o mesmo assenta na análise e avaliação do risco de segurança de informação, o que é especialmente verdade na avaliação dos riscos associados aos incidentes de segurança de informação. Contudo, se o QNRCS estabelece a adoção de um conjunto de controlos, é porque estes controlos visam mitigar riscos, e não são apenas riscos associados a incidentes, mas sobretudo a riscos de negócio.

Assim, assumindo o processo de Gestão de Risco como o coração da implementação e possível certificação do QNRCS, é justo afirmar que a adequação dos controlos (subcategorias do QNRCS) e dos seus graus de maturidade, não deve ser igual para todas as organizações, mas sim em função da sua aceitação de risco, pelo que poderão existir casos em que certas subcategorias não se apliquem a algumas organizações, ou que o seu risco não justifique um grau de maturidade intermédio ou avançado em determinada subcategoria. No entanto, é importante ter em mente que o QNRCS tem 5 objetivos[76], e que se uma organização que pretende ser certificada no QNRCS[77], não pode demitir de cumprir com todas as categorias.

É de notar também que, pelo facto de as organizações mais pequenas possuírem uma superfície de ataque mais reduzida, a probabilidade de serem alvo de um ciberataque também é mais reduzida, o que pode justificar uma exigência na maturidade menor.

Das lições aprendidas da implementação do QNRCS na organização, destacam-se as seguintes:

- Flexibilidade é chave numa pequena empresa.
- O processo mais eficiente (relação custo / benefício) de segurança de informação é a implementação de ações de formação e sensibilização. De facto, o vetor de ataque mais explorado é o fator humano e este é também aquele que, se treinado, constitui a melhor linha de defesa.
- Processos de análise forense revelam-se dos mais difíceis de implementar devido ao seu alto nível de especialização, facto que provavelmente obrigará PMEs a recorrerem a serviços externos de SOC.
- Numa ótica de esforço humano, a implementação de novos processos e tecnologias traduz-se inevitavelmente num aumento da carga de trabalho dos colaboradores da organização, mesmo que alguns processos novos consigam simplificar processos já existentes. Assim, muito provavelmente será necessário um reforço do pessoal para gerir novos processos ou operar novas ferramentas, para além de operar as já existentes. Contudo, a complexidade destes processos nas pequenas e microempresas são menores do que nas médias ou grandes organizações. Isto pode permitir que a exigência de conhecimentos necessários não seja tão exigente e que,

[76] Identificar, Proteger, Detetar, Responder e Recuperar
[77] Num cenário hipotético de certificação do QNRCS.

por conseguinte, seja possível concentrar alguns processos de áreas distintas nas mesmas pessoas (exemplo: Gestão de Risco com Gestão de Alterações). Porém, alguns processos poderão não permitir esta simplificação, tal como a monitorização de sistemas, a qual necessita de alguém especializado em segurança e redes que consiga interpretar os dados apresentados pelo sistema. Acumula-se ainda a questão da procura, já que como vimos na Introdução desta tese, Portugal possui muitas vagas de IT por preencher e a implementação destas normas aumentaria ainda mais a procura por profissionais da área, tendo em conta que nem todos os profissionais de IT são de segurança.

- As implementações sugeridas nesta tese inserem-se num cenário em que a organização possui um espaço próprio (um ou vários escritórios ou até mesmo instalações dedicadas como armazéns, prédios, etc..), mas nem sempre é o caso. Muitas organizações de pequena e micro dimensão garantem a sua atividade a partir de espaços partilhados com outras organizações, pelo que carecem da autonomia necessária para criarem processos de controlo de acessos bem como garantirem instalações de servidores e outras máquinas físicas em locais seguros.
- Do ponto de vista financeiro, a aquisição destes recursos – humanos e técnicos – poderá representar um grande encargo para as micro e pequenas empresas. Tipicamente, este tipo de organização tende a concentrar o seu investimento em recursos que tenham um impacto direto na sua faturação e no seu negócio.

Apesar dos constrangimentos identificados e atendendo ao principio hipotético de que uma organização pode adequar a sua implementação do QNRCS ao seu apetite ao risco, esta tese concluiu que é possível uma PME posicionar-se em conformidade com o QNRCS. Através da adoção de processos eficientes, materiais didáticos institucionais, serviços externos e tecnologia *open source*, as PMEs conseguem assumir uma postura de cibersegurança que lhes permitirá reduzir o risco de negócio, garantir a conformidade com o QNRCS e garantir um crescimento saudável e seguro.

6.2. Observações acerca dos critérios de conformidade

Conforme foi referido acima, não existem atualmente critérios de conformidade com QNRCS, e as propostas desta tese para a conformidade tiveram 3 princípios em mente:

1. A maturidade das subcategorias deve-se adequar ao Risco da organização,
2. Os 5 objetivos e as 23 categorias do QNRCS devem ser garantidos,
3. Nem todas as subcategorias devem ser impostas.

Adicionalmente, a adoção de um sistema de pontos associado ao grau de maturidade de cada subcategoria, confere flexibilidade ao processo de Gestão de Risco e Gap Analysis do QNRCS, permitindo também o rastreamento temporal dos graus de maturidade das subcategorias, dando assim uma visibilidade da melhoria contínua inerente ao QNRCS.

Todavia, apesar do QNRCS referir diversas vezes processos de melhoria contínua, não refere nem dá orientações referentes a indicadores de performance (KPI) que permitam aferir a eficácia dos controlos, ou da adequação dos critérios de classificação de risco – será que a política de backups é a mais adequada? Será que as quantificações do impacto e da probabilidade são as mais adequadas?

Neste sentido, pode ser justo afirmar que o QNRCS beneficiaria de métricas ou orientações relativas a indicadores de performance.

É interessante constatar que o QNRCS também toca noutras regras de segurança de informação. Note-se que a lei nº 46/2018 estabelece um regime jurídico da segurança do ciberespaço, no qual declara obrigatória a implementação de "medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação" nas seguintes entidades:

a) Administração Pública;
b) Aos operadores de infraestruturas críticas;
c) Aos operadores de serviços essenciais;
d) Aos prestadores de serviços digitais;
e) A quaisquer outras entidades que utilizem redes e sistemas de informação

Assim, apesar do carácter voluntário (atual) de implementação do QNRCS, o mesmo assume-se como um guia de cibersegurança que visa responder às obrigatoriedades da lei nº 46/2018.[78] Deste modo, podemos assumir que apesar de nem todos os pontos serem de implementação obrigatória, o completo cumprimento do QNRCS assegura o total cumprimento da lei. Adicionalmente, é de referir que ao abrigo do Regulamento Geral de Proteção de Dados, a Resolução de Conselho de Ministros 41/2018 prevê a implementação de um conjunto de medidas técnicas respeitantes à arquitetura de segurança de redes e sistemas de informação de serviços e entidades da Administração direta e indireta do Estado.79 Ou seja, algumas das obrigações da RCM 41/2018 coincidem com alguns dos requisitos do QNRCS, (por exemplo: controlo de acessos a aplicações ou gestão de passwords). Este facto constitui mais um indício de que o cumprimento do QNRCS também cobre aspetos legais de outras normas.

[78] De acordo com o sumário executivo do Quadro Nacional de Referência para a CiberSegurança: "Em alinhamento com a Lei n.º 46/2018, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, este documento tem como missão providenciar às organizações um guia de cibersegurança que sistematiza um conjunto de medidas para as problemáticas mais relevantes da atualidade nesta matéria. Pretende disponibilizar as bases para uma organização cumprir os requisitos mínimos de segurança da informação recomendados."

[79] A RCM 41/2018 refere: "Nos termos da alínea g) do artigo 199.º da Constituição, o Conselho de Ministros resolve: 1 — Aprovar os requisitos técnicos mínimos das redes e sistemas de informação que são exigidos ou recomendados a todos os serviços e entidades da Administração direta e indireta do Estado, os quais constam do anexo à presente resolução e que dela faz parte integrante."

Da constatação anterior percebe-se que se uma micro ou pequena empresa ambicionar prestar algum serviço digital ao Estado Português, ou operar serviços críticos ou essenciais ou simplesmente serviços digitais, deverá cumprir com pelo menos uma parte do QNRCS. Além disso, como muitos dos processos recomendados no próprio QNRCS são escaláveis, a sua correta e total implementação permite às organizações que a implementam, garantir um crescimento estruturado da sua infraestrutura minimizando assim o risco de falha de segurança em todo o seu processo.

6.3. Observações relativas aos graus de maturidade

Os graus de maturidade das subcategorias foram pela primeira vez definidos no Quadro de Avaliação, e tal como referido na secção anterior (7.2), este trabalho académico visou atribuir valores para os diferentes graus de maturidade das subcategorias.

No entanto, algumas subcategorias não possuem grau Inicial[80] (ex: DE.AE1) e outras não possuem grau Inicial nem Intermédio (RS.ME1), o que, á luz do sistema de pontos definidos nesta tese, pode interferir com as contas relativas às conformidades (ex: gestor de risco atribuir 2 pontos – grau intermédio – na subcategoria RM.ME1, quando o único grau correspondente a qualquer forma de controlo é o grau Avançado). De igual forma, a subcategoria DE.AE1 beneficiaria da definição de um grau Inicial.

6.4. Trabalho futuro

A título de trabalho futuro, valerá a pena debruçar-se sobre uma metodologia de gestão de risco baseada no setor, dimensão, área de atividade e outras varáveis, de modo a se agilizar e orientar as empresas a definir a estratégia de gestão de risco, e consequentemente o grau de maturidade alvo do QNRCS.

6.5 Nota Final

É inquestionável a necessidade de as organizações nacionais adotarem uma postura defensiva face às ameaças globais à segurança de informação. Estas ameaças não só constituem um problema às próprias organizações, como também constituem um problema para a sociedade portuguesa em geral, porque à semelhança de outras ameaças não digitais (como a do vírus Covid-19), a solução do problema não depende apenas de decisões políticas, mas depende sobretudo de uma resposta eficaz da sociedade civil. E se na Introdução deste trabalho foi evocado o aspeto de "imunidade de grupo" necessária à sociedade para fazer frente a esta nova realidade geopolítica, é porque tal medida é crucial para a defesa dos interesses dos cidadãos como também da nação como um todo.

[80] Ou Básico, conforme designado nesta tese de mestrado.

Face à existência de várias normas de segurança existentes atualmente (NIST, ISO 27001, outras…) e de normas de gestão de IT (ITIL, COBIT e mais), acresce a necessidade de se criar uma orientação comum que dissipe possíveis dúvidas relativamente a qual das opções seguir. E de facto o QNRCS reúne boas práticas de gestão de IT como segurança de informação, pelo que desta forma preenche inteiramente esta necessidade.

Por fim, a segurança é algo que só tem visibilidade quando falha, e em tempos de conturbação económica, a sua relevância é invariavelmente relegada para 2º plano. Contudo, tal como outros flagelos da sociedade, o cumprimento das regras e boas práticas de segurança são-nos recomendadas para nos proteger e aos que estão a nosso cargo de ameaças de inimigos invisíveis, algo que infelizmente, começa-se a tornar recorrente no século XXI.

Bibliografia

Bibliografia Digital

[1] Centro Nacional de Cibersegurança, (2019), Quadro Nacional de Referência em Cibersegurança, disponível em: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

[2] Centro Nacional de Cibersegurança, (2019), Quadro de Avaliação de Capacidades de Cibersegurança Disponível em https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf

[3] Secretaria de Estado da Transição Digital, página institucional, disponível em: https://www.portugal.gov.pt/pt/gc22/area-de-governo/economia-transicao-digital/secretarios-de-estado

[4] Centro Nacional de Cibersegurança, (2019), Relatório Riscos e Conflitos do Centro Nacional de Cibersegurança, disponível em: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurança-cncs.pdf

[5] Instituto Nacional de Estatística, Proportion of enterprises using information and communication technologies (%) by Employment size class and Type of technology (information and communication); Annual, disponível em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_indicadores&indOcorrCod=0007991&contexto=bd&selTab=tab2

[6] Thales, (2019), Threat Report, disponível em: https://www.thalesesecurity.com/2019/data-threat-report-thankyou

[7] Governo de Portugal, (2018), Relatório anual de Segurança Interna 2018, disponível em: https://www.portugal.gov.pt/pt/gc21/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-2018

[8] IBM (2021), Cost of a data breach Report 2021, disponível em : https://www.ibm.com/security/data-breach

[9] Pordata (2021), Pequenas e médias empresas em % do total de empresas: total e por dimensão, disponível em: https://www.pordata.pt/Portugal/Pequenas+e+m%C3%A9dias+empresas+em+percentagem+do+total+de+empresas+total+e+por+dimens%C3%A3o-2859

[10] Dashlane (2018), Databreaches blog, disponível em: https://blog.dashlane.com/data-breaches-2018/

[11] Economia e Finanças (2016), Definição de Grande Empresa, Média Empresa, Pequena Empresa e Microempresa, disponível em: https://economiafinancas.com/2016/definicao-grande-media-pequena-microempresa/

[12] Ottis (2008), Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, NATO Cooperative Cyber Defence Centre of Excellence, disponível em: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[12] ISACA, COBIT Framework, disponível em: https://www.isaca.org

[13] ISO Foundation (2013), ISO/IEC 27001, disponível em: https://www.iso.org/isoiec-27001-information-security.html

[14] NIST (2018), Cybersecurity Framework Version 1.1, disponível em: https://www.nist.gov/cyberframework/framework

[15] OpenVAS, Open Vulnerability Assessment Scanner, disponível em: https://www.openvas.org/

[16] Sullo, Nikto, Github, disponível em: https://github.com/sullo/nikto

[17] Udemy, Online Courses, disponível em: www.udemy.com

[18] Cybrary, Free cybersecurity Training and Career Development, disponível em: www.cybrary.com

[19] SANS, Security Policy Templates, disponíel em: https://www.sans.org/information-security-policy/?page=5

[20] Rede Nacional CSIRT, disponível em: https://www.redecsirt.pt/

[21] Hong Kong Goverment Infosec, disponível em: https://www.infosec.gov.hk/en/

[22] Whatsapp, disponível em: https://www.whatsapp.com/

[23] Telegram, disponível em: https://telegram.org/

[24] Signal, disponível em: https://signal.org/en/

[25] Instituto Nacional de Estatística, Information and knowledge society - household survey, disponivel em: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=415621509&DESTAQUESmodo=2

[26] Associação da Economia Digital, Estudo Economia Digital 2020, disponível em: https://www.acepi.pt/pt/estudos/

Bibliografia escrita

[25] Deveza, J. N. (s.d.). *1509.*

[26] Deveza, J. N. (s.d.). *Portugal: Pioneiro da Globalização.*

[27] Jorge Miranda. Curso de Direito Constitucional 1.Estado e Constitucionalismo. Constituição. Direitos Fundamentais