PM

Segurança e Auditoria em Sistemas de Informação e Comunicação

Implementação numa entidade pública

PROJETO DE MESTRADO

Carla Margarida Rocha Carvalho

MESTRADO EM ENGENHARIA INFORMÁTICA

UNIVERSIDADE da MADEIRA

A Nossa Universidade

www.uma.pt

novembro | 2018

Segurança e Auditoria em Sistemas de Informação e Comunicação

Implementação numa entidade pública

PROJETO DE MESTRADO

Carla Margarida Rocha Carvalho
MESTRADO EM ENGENHARIA INFORMÁTICA

ORIENTADOR
Eduardo Miguel Dias Marques

“There are risks and costs to action.

But they are far less than the long-range risks of comfortable inaction.”

(John F. Kennedy)

AGRADECIMENTOS

A realização deste projeto de mestrado é o culminar de uma importante etapa da minha vida e contou com apoios e incentivos decisivos, pelos quais desejo exprimir o meu sincero reconhecimento.

À IHM – Investimentos Habitacionais da Madeira, EPERAM, nomeadamente ao Conselho de Administração, à Direção Financeira e Administrativa e ao Serviço Administrativo, nas pessoas do Dr. Ruben Nunes, do Dr. Dionísio Pita e do Dr. José Carlos Dias, respetivamente, pela aprovação da realização deste trabalho, pela disponibilidade, confiança, apoio e por me proporcionarem as condições para esta concretização.

Ao Professor Doutor Eduardo Marques, meu orientador, registo com elevada consideração a oportunidade que me deu de realizar este trabalho, além da valiosa colaboração, orientação exemplar, rigor científico, revisão crítica e oportuna, partilha de conhecimento e disponibilidade manifestada desde o primeiro momento.

À minha família, pela sólida presença e apoio incondicional que sempre me deram. Um agradecimento muito especial à minha madrinha Manuela, pela inestimável amizade, generosidade, conselhos e incentivo para este percurso académico.

Aos amigos de longa data, pelo apoio, confiança, força, alegria e ânimo que me transmitiram ao longo desta jornada.

Aos meus colegas e a todos os que, não estando aqui referidos, de alguma forma me apoiaram e contribuíram para que a realização deste trabalho fosse possível.

A todos reitero o meu apreço e agradecimento.

RESUMO

O incremento da produção de informação digital, os desafios à comunicação segura e à manutenção e salvaguarda dos dados estão a par com o aumento da criminalidade informática manifestada através de técnicas de intrusão e aproveitamento de vulnerabilidades. Este cenário impõe às empresas a realização de melhorias aos paradigmas da segurança, sob pena de verem comprometido um bem fundamental à sua própria existência: a *INFORMAÇÃO*.

Para melhor enfrentar os perigos e desafios da presença no ciberespaço, pretendeu a empresa pública Investimentos Habitacionais da Madeira, EPERAM (IHM) analisar e elevar o nível de segurança da informação e das comunicações seguindo as boas práticas desta área, pois, não obstante os procedimentos já aplicados, os eventos de segurança são ainda abordados maioritariamente a jusante e de forma reativa.

Investigado o estado da arte sobre normas, *frameworks* e certificações para a segurança da informação, consultada legislação relacionada e realizada uma análise à situação atual da empresa, foi proposta uma metodologia, fundamentada na gestão do risco, para o estabelecimento, implementação, manutenção e melhoria, de forma contínua, de um sistema de gestão de segurança da informação, através de um conjunto de 18 processos com enquadramento na norma NP ISO/IEC 27001:2013. Paralelamente, para garantir a sua sustentabilidade, foi aplicado o ciclo contínuo PDCA, que foi útil para que os controlos de segurança pudessem ser já implementados e medidos. Foi incorporada na metodologia proposta a norma NIST SP 800-61r2, com 4 processos, pela especificidade no campo da gestão de incidentes.

A implementação resultou na definição de 8 políticas, acompanhadas de 47 controlos de segurança, dos quais 37 foram medidos. Os resultados permitiram identificar as melhorias necessárias mais prementes através de um esquema de cores. O recurso ao modelo corporativo de governança e gestão de tecnologias de informação - COBIT 5 - contribuiu para a realização posterior de uma análise à capacidade dos processos e aferição da sua maturidade.

PALAVRAS-CHAVE

Segurança da informação; Gestão de risco; Norma ISO/IEC 27001:2013; Políticas de segurança; Segurança de operações; Segurança em comunicações; Norma NIST SP 800-61r2; Gestão de incidentes; Framework COBIT 5; RGPD; Auditoria;

ABSTRACT

The increase in the production of digital information, the challenges to communication's security and to the maintenance and safeguarding of data are in line with the increase in computer crime manifested through intrusion techniques and exploitation of vulnerabilities. This scenario imposes on companies the realization of improvements to the security paradigms, under penalty of being compromised a fundamental asset to their own existence: *INFORMATION*.

To better face the dangers and challenges of the presence in cyberspace, the public company Investimentos Habitacionais da Madeira, EPERAM (IHM) intended to analyze and raise the level of information and communications security following good practices in this area, since, despite the procedures already applied, security events are still mostly addressed downstream and reactively.

After an investigation to the state of the art on norms, frameworks and certifications for information security, the examination of related legislation and the carried out an analysis to the current situation of the company, a methodology, based on risk management, was proposed for the establishment, implementation, maintenance and improvement in a continuous way, of an information security management system, through a set of 18 processes covered by the NP ISO/IEC 27001:2013 standard. In parallel, to ensure its sustainability, the PDCA continuous cycle was applied, which was useful so that the safety controls could be already implemented and measured. The NIST SP 800-61r2 standard was incorporated into the proposed methodology, with 4 processes, for its specificity in the field of incident management.

The implementation resulted in the definition of 8 policies, accompanied by 47 safety controls, of which 37 were measured. The results allowed the identification of the necessary improvements through a color scheme. The use of the corporate governance and information technology management model - COBIT 5 - contributed to the subsequent accomplishment of an analysis of the processes' capacity and measurement of their maturity.

KEYWORDS

Information security; Risk management; ISO/IEC 27001:2013 Standard; Security policies; Security of operations; Security in communications; NIST SP 800-61r2; Incident management; COBIT 5 Framework; GDPR; Audit;

ÍNDICE

SIGLAS E ACRÓNIMOS

(ISC)²	*International Information System Security Certification Consortium*
AP	*Access Point*
CA	Conselho de Administração
CCSP	*Certified Cloud Security Professional*
CEH	*Certified Ethical Hacker*
CEN	*European Committee for Standardization*
CERT	*Computer Emergency Response Team*
CISA	*Certified Information Systems Auditor*
CISM	*Certified Information Security Manager*
CISSP	*Certified Information Systems Security Professional*
CND	*Certified Network Defender*
COBIT	*Control Objectives for Information and related Technology*
CompTIA	*Computing Technology Industry Association*
CRISC	*Certified in Risk and Information Systems Control*
DMZ	*Demilitarized Zone*
DNS	*Domain Name System*
DNSSEC	*Domain Name System Security Extensions*
EC-Council	*International Council of Electronic Commerce Consultants*
ENISA	*European Union Agency for Network and Information Security*
GAC	Gabinete de Assessoria e Comunicação
GIAC	*Global Information Assurance Certification*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IHM	Investimentos Habitacionais da Madeira, EPERAM
IP	*Internet Protocol*
IPQ	Instituto Português da Qualidade, I.P.
IPS	*Intrusion Prevention System*
ISACA	*Information Systems Audit and Control Association*

ISO	*International Organization for Standardization*
MAC	*Media Access Control (Address)*
NIST	*National Institute of Standards and Technology*
NP	Norma Portuguesa
NTP	*Network Time Protocol*
OUI	*Organizationally Unique Identifier*
RAM	Região Autónoma da Madeira
RGPD	Regulamento Geral de Proteção de Dados
RFC	*Request for Comments*
SANS	*System Administration, Networking, and Security Institute*
SDN	*Software-Defined Network*
SGSI	Sistema de Gestão de Segurança da Informação
SIEM	*Security Information and Event Management*
SLA	*Service Level Agreement*
SSH	*Secure Shell*
SSID	*Service Set Identifier*
TI	Tecnologias de Informação
UE	União Europeia
VLAN	*Virtual Local Area Network*

LISTA DE FIGURAS

LISTA DE TABELAS

1. INTRODUÇÃO

Com o advento da Internet assistimos nas últimas décadas a uma revolução na forma como cidadãos e empresas passaram a interagir e a desenvolver atividades no mundo virtual denominado ciberespaço. As empresas, motivadas por acréscimos de eficiência, competitividade, proximidade com os clientes, redução de custos, entre outros objetivos, têm investido na criação de infraestruturas de rede e comunicações para suporte aos sistemas informáticos, como é o caso das redes em fibra ótica, e no desenvolvimento aplicacional para disponibilização de serviços, nomeadamente através de aplicações para dispositivos móveis, impulsionando desta forma as suas atividades e alargando o seu espaço de atuação. Já os cidadãos têm visto nascer novos ambientes virtuais, tais como as redes sociais e aplicações baseadas em realidade aumentada, assim como a possibilidade de usufruírem de múltiplos serviços prestados *online*, cujos benefícios, em última instância, refletem-se na sua qualidade de vida.

O ciberespaço, caracterizado por uma grande diversidade de dispositivos interligados em redes de dados cada vez mais velozes e por organizações e utilizadores progressivamente exigentes, não deixa, contudo, de revelar fragilidades cuja origem remonta à própria conceção da Internet, na medida em que os seus fundadores "preocuparam-se com intrusões e ameaças militares, mas não anteciparam que os utilizadores da rede se atacassem mutuamente" [1]. Assim, não raras vezes, vemos noticiadas publicamente intrusões, roubo de dados, interceções em comunicações, negação de serviços ou ataques a servidores de empresas, públicas e privadas, e em diversa escala. Entre as principais ameaças identificadas em 2017 pela Agência Europeia para a Segurança das Redes e da Informação (ENISA) encontram-se o *malware*, os ataques baseados na *Web*, os ataques a aplicações *Web*, o *phishing* e o *spam* [2, p. 90].

Os ataques cibernéticos, cada vez mais numerosos, sofisticados e planeados para causar o máximo impacto, continuam a ter na geração de receitas um dos seus principais objetivos, sendo este facto confirmado pela *Information Systems Audit and Control Association* (ISACA) no relatório sobre o estado da cibersegurança para 2018 [3, p. 7]. Em Portugal, o Relatório Anual de Segurança Interna 2017 confirma esta tendência, sendo que 17% dos incidentes analisados e resolvidos pelo Centro Nacional de Cibersegurança afetaram direta ou indiretamente entidades do Estado, representando um acréscimo de 8% em relação ao ano transato [4, p. 154].

Pelo valor e papel estratégico que desempenha nas empresas, a *INFORMAÇÃO* tornou-se um dos alvos preferenciais dos ataques no ciberespaço. Seja através de pedidos de resgate na sequência de infeções por *ransomware,* pela criação de *botnets* para infeção de computadores em redes e posterior controlo para fins de recolha de informação ou ataques de negação de serviços, os ciberataques são perpetrados por indivíduos aptos a explorar lacunas de segurança e vulnerabilidades em dispositivos e redes, muitas vezes conhecidas e para as quais já existem correções, deixando exposta a incorreta abordagem das empresas aos problemas de segurança.

Desafios importantes colocam-se, também, quanto à proteção contra vulnerabilidades ainda não identificadas (*zero-day*) e à expansão da denominada Internet das Coisas (IoT – *Internet of Things*), com um crescente número de dispositivos ligados à rede pública de dados e cuja visão "é permitir que as coisas sejam conectadas a qualquer hora, em qualquer lugar, com qualquer coisa e qualquer um, idealmente utilizando qualquer caminho, rede e serviço" [5, p. 2]. Acrescem assim os riscos de segurança para a privacidade dos utilizadores, a confidencialidade das comunicações e a gestão de autenticação. Estes dispositivos representam vetores de ataque adicionais para os quais a resposta humana poderá não ser suficiente e que requerem soluções capazes de prevenir, tanto quanto possível, disrupções na atividade das empresas.

Não menos relevantes são os domínios da segurança do *software* aplicacional e o seu desenvolvimento seguro, a segurança das bases de dados, assim como o recurso a soluções na nuvem onde "a segurança é a principal preocupação que dificulta a adoção do modelo de computação" [6, p. 1]. A segurança da cadeia de fornecimento é, assim, fundamental para garantir a continuidade do serviço. Em todos estes casos, a ausência de políticas de segurança ou a sua não monitorização e revisão permanentes contribui largamente para o aumento do risco.

É, pois, fundamental que as empresas não se permitam adotar procedimentos avulsos na gestão do risco de segurança da informação, mas sejam antes capazes de preservar as suas informações, manter os seus sistemas atualizados e ambicionar a excelência nos procedimentos de segurança para salvaguarda do seu património, da sua reputação e, acima de tudo, da sua própria existência. Um exemplo de procedimento é a implementação de uma política de segurança de rede que não permita a utilização de equipamentos de rede que não sejam propriedade da empresa, de modo a evitar intrusões indevidas nos sistemas. Este controlo garante que as ligações existentes são monitorizadas internamente, permitindo ações de mitigação (e.g. através de bloqueio de porta específica) sempre que sejam detetadas anomalias.

Orçamentos limitados e outros constrangimentos, como a escassez de recursos qualificados em segurança informática, a resistência à mudança ou a influência cultural afetam a capacidade das empresas de implementar os mecanismos necessários à defesa das suas infraestruturas. Em caso de ataque, as decisões de segurança são normalmente conduzidas pela necessidade de resposta imediata ao incidente e não por uma abordagem holística à segurança baseada no risco. Este cenário revela uma postura reativa, não recomendável, oposta a uma ação proactiva de planeamento a longo prazo. Como referido por H. São Mamede [2, p. 20], "organizações que optem por uma postura reativa, abordando a segurança apenas após a ocorrência de ataques, arriscam-se a enfrentar a inevitabilidade do seu próprio fim".

As limitações mencionadas, nomeadamente as derivadas de parcos recursos financeiros, não são, no entanto, impeditivas da adoção e implementação de muitas das melhores práticas de segurança da informação, resultantes de inúmeras concretizações, provas e melhorias ao longo dos anos, que se encontram documentadas e à disposição dos serviços públicos e sectores empresariais em normas, modelos, regulamentos e documentos afins. Segundo a consultora internacional *Gartner Inc.*, é estimado que os custos das empresas com a segurança

da informação venham a aumentar significativamente, atingindo os 113 mil milhões de dólares em 2020 [8]. Torna-se, pois, imperativo que as empresas, face às reais ameaças a que estão sujeitas, identifiquem e avaliem o seu património digital e detetem os seus pontos fracos no que respeita à gestão de segurança, pois só com base nesse conhecimento será possível aferir o risco associado, estimar os custos e definir as medidas de prevenção adequadas à sua minimização. De salientar que, neste contexto, a análise de custo apenas faz sentido considerando também o benefício associado, e não de forma isolada, pois o investimento em segurança não deve ser superior ao valor dos bens a proteger.

A gestão da segurança da informação exige uma visão ampla e integrada de vários domínios, entre os quais o dos recursos humanos. A máxima atenção deve ser dada aos utilizadores e aos privilégios de acesso a estes atribuídos, assim como à necessidade de os informar sobre as suas responsabilidades sempre que acedem à rede e à informação disponibilizada através de aplicações informáticas. Na maioria dos casos, os utilizadores não possuem os conhecimentos suficientes para lidar corretamente com questões de segurança, pelo que compete às empresas capacitá-los para lidar com o risco e acautelar que os sistemas estão preparados para as suas ações. Uma das soluções é através da definição de arquiteturas cumpridoras do princípio *"security by design*", que considera a segurança ao longo do ciclo de vida do *software* e do *hardware*, tal como é exigido no Regulamento Geral de Proteção de Dados[1] [9], lei que responsabiliza e penaliza fortemente as organizações que, tendo na sua posse dados pessoais de utilizadores, clientes ou outras entidades, não sejam capazes de demonstrar a garantia da sua segurança.

A informação, como um dos bens mais valiosos de qualquer empresa, funde-se, atualmente, com o seu próprio funcionamento. Não é possível a normal operação de uma organização se não houver a garantia de esta estar a ser executada com base em informação atual, fidedigna e sempre disponível. Como tal, a gestão da segurança da informação impõe-se como fator crítico subjacente à gestão da própria empresa. Idealmente, é desejável que as empresas disponham de um sistema de gestão de segurança da informação que inclua a definição de uma política de segurança e imponha a implementação de mecanismos capazes de cobrir e assegurar os principais aspetos da segurança: a confidencialidade, a integridade, a disponibilidade, a autenticidade, o controlo de acesso e a não repudiação.

De igual forma, o conhecimento dos processos de auditoria e dos requisitos para certificação permite às empresas se adaptarem no sentido de convergir a sua operação para a obtenção do reconhecimento proporcionado por estes mecanismos.

É este o desígnio do presente trabalho, em que se pretende analisar a situação atual na empresa Investimentos Habitacionais da Madeira, EPERAM (IHM), identificar o problema que possa estar a causar riscos à segurança da informação, procurar através do estado da arte uma metodologia útil e adequada à sua resolução, implementá-la e aferir os resultados no sentido de validar a opção tomada.

[1] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Em cumprimento com a condição de garantia de confidencialidade solicitada pelo Conselho de Administração da IHM, deste trabalho consta a documentação que consubstancia a análise efetuada, sendo omissos os detalhes técnicos sobre os controlos aplicados e a indicação do estado real do projeto.

1.1. MOTIVAÇÃO

A motivação para a realização deste projeto surgiu da perceção de haver a necessidade de efetuar melhorias na IHM ao nível da segurança da informação digital e das comunicações de forma a reforçar os mecanismos existentes e a elevar a qualidade do serviço informático, adaptando-o simultaneamente às crescentes exigências de conformidade legal.

Neste sentido, utilizou-se a oportunidade proporcionada pelo mestrado para tentar resolver situações que ao longo do tempo se tornaram evidentes, nomeadamente a ausência de políticas e de procedimentos detalhados que dão origem a que os técnicos, apesar da sua experiência, executem as tarefas informáticas de forma tácita, podendo incorrer em configurações incompletas, terminologias e *inputs* incoerentes, falta de documentação e falhas na aplicação de mecanismos necessários ao bom funcionamento dos sistemas, e como tal representam riscos acrescidos para a segurança da informação.

A resolução deste problema é importante para a IHM pois permitirá melhorar os procedimentos atuais de proteção da informação, reforçar a robustez dos sistemas e das comunicações e assim debelar um conjunto de riscos, com reflexo nos serviços prestados interna e externamente e na reputação da empresa.

1.2. OBJETIVOS

Tendo sido percecionada a necessidade de melhorias nos procedimentos de segurança informática instituídos na IHM, o projeto ora apresentado tem como principal objetivo propor uma arquitetura com processos e políticas de segurança para os sistemas de informação e comunicação desta empresa.

Pretende-se, numa primeira fase, caracterizar a IHM em termos de segurança, analisando diversos contextos quanto ao nível de segurança existente. Em concreto, esta análise à situação atual passa por compreender se os processos empregues na gestão dos sistemas de informação e das comunicações são os adequados. Este tipo de análise permite obter uma visão abrangente da empresa, por incluir levantamentos de dados sobre espaços físicos e condições ambientais, bens tecnológicos, categorização do pessoal, topologia de rede e ambiente aplicacional, assim como sobre os processos existentes.

É com base neste retrato da IHM que será possível identificar lacunas e aferir se os processos atuais requerem ajustamentos para melhoria da sua eficiência e eficácia. Propor-se-á, então,

uma arquitetura que se creia ser a que apresente opções de segurança com mais vantagens para a empresa, partindo-se em seguida para a definição de um plano de implementação.

Deste plano constarão os processos necessários ao estabelecimento da arquitetura proposta, a ordem de implementação de cada processo, assim como a identificação dos instrumentos utilizados e produzidos, entre os quais devem constar os registos documentais.

Para se poder avaliar as opções de segurança escolhidas serão estabelecidos indicadores de desempenho para medição de resultados. A análise de cada resultado permitirá verificar se a opção tomada é válida e posteriormente concluir sobre a adequabilidade da arquitetura.

Estabelecidos estes objetivos para o projeto, acredita-se estarem reunidas as condições para, em caso de avaliação positiva, a IHM poder ver concretizada a aplicação de práticas de referência na gestão da segurança da sua infraestrutura informática, cenário este que oferece melhor sustentação perante ameaças e ataques e que releva a imagem e o nome da empresa, passando a estar mais próximo o alcance de objetivos de certificação.

Em resumo, os objetivos do projeto são:

- Caraterizar a IHM em termos de segurança.
- Propor uma arquitetura com processos e políticas.
- Avaliar as propostas de melhoria através de implementação e medição de indicadores de desempenho.

1.3. ESTRUTURA DO DOCUMENTO

O presente documento encontra-se estruturado em seis capítulos, que na sequência se resumem:

No primeiro capítulo é introduzida a temática da segurança informática, os ciberataques e os desafios que a presença no ciberespaço coloca às empresas. São expostos a motivação para a realização deste projeto, os objetivos globais a atingir e enunciados os capítulos que compõem a estrutura do presente documento.

O estado da arte, abordado no capítulo 2, apresenta a norma NP ISO/IEC 27001:2013, principal norma da família ISO/IEC 27000, sobre o estabelecimento, a implementação, a manutenção e a melhoria contínua de um sistema de gestão de segurança da informação. Identificam-se características que o tornam uma mais-valia, nomeando-se alguns dos desafios à sua implementação e fatores determinantes para o sucesso. São também abordadas outras normas da mesma família que ajudam na aplicação da norma principal, modelos presentes em certificações e legislação com implicações na segurança de dados.

No capítulo 3 é apresentada a empresa IHM - Investimentos Habitacionais da Madeira, EPERAM, a sua estrutura orgânica e um sumário das áreas de atividade, especificando-se a

situação atual no contexto das tecnologias de informação e comunicação e o problema ao qual este trabalho pretende dar resposta.

O quarto capítulo apresenta a análise e metodologia proposta para a resolução do problema através de uma representação gráfica dos processos envolvidos e das interligações entre estes, assim como uma descrição detalhada de cada um dos processos.

No capítulo 5 é descrito o processo de implementação e são apresentados os indicadores de desempenho cuja medição permite obter resultados para realização de análise crítica.

Por fim, no capítulo 6, apresenta-se as conclusões sobre a adequabilidade da metodologia adotada, nomeadamente se a sua aplicação permitiu melhorar a situação descrita como problema. São também abordados os desafios e limitações encontradas, propondo-se um conjunto de recomendações para trabalho futuro.

Na sequência introduz-se o capítulo sobre o estado da arte, no qual são apresentadas e comparadas normas relevantes e específicas no âmbito da segurança da informação.

2. ESTADO DA ARTE

Abordados os desafios que as empresas enfrentam pela sua presença no ciberespaço, e definido o objetivo principal de se encontrar uma solução de melhoria da gestão da segurança da informação e das comunicações na empresa Investimentos Habitacionais da Madeira, EPERAM (IHM), procedeu-se à análise de trabalho relacionado de forma a obter os alicerces teóricos para tratar o tema e o problema e, concomitantemente, fazer o ponto de situação sobre o mais alto nível de desenvolvimento desta área de conhecimento.

A informação digital reside maioritariamente em bases de dados e outros sistemas de armazenamento local nas empresas, ou em sistemas distribuídos, incluindo na nuvem, sendo transmitida através de sistemas de comunicação que incluem cablagem, dispositivos de gestão das comunicações e um funcionamento lógico de transporte de dados nas redes até chegar aos utilizadores finais. Garantir a segurança da informação e de todos os sistemas envolvidos passa por garantir os seus princípios fundamentais: confidencialidade, integridade, disponibilidade, autenticidade, controlo do acesso e não repudiação.

Gerir eficazmente a segurança da informação implica dispor de capacidade para determinar quais os controlos necessários à adequada gestão de todos os sistemas que lidam com informação. Estes sistemas não se limitam apenas aos sistemas informáticos, porquanto o acesso à informação, além de ocorrer de forma lógica através das aplicações informáticas e das redes de dados, pode também ser feito fisicamente, o que implica a existência de controlos de acesso a áreas críticas, entre outros requisitos. Além de determinar quais os controlos necessários, a gestão da segurança da informação incide particularmente na forma como estes controlos devem ser aplicados, monitorizados e melhorados.

Neste sentido, uma série de normas, *frameworks*, certificações, regulamentos e outros instrumentos são utilizados para a escolha desses controlos, escolha esta que deve atender particularmente ao estado da informação, ou seja, se os dados estão armazenados ou em movimento. No seguimento, e sobre cada um destes recursos, apresenta-se o conceito e o entendimento sobre as suas mais-valias.

Segundo o *European Committee for Standardization* (CEN), "uma norma é um documento técnico projetado para ser usado como uma regra, diretriz ou definição. As normas são criadas reunindo todas as partes interessadas, tais como fabricantes, consumidores e reguladores de um material, produto, processo ou serviço específico. Todas as partes beneficiam da normalização através do aumento da segurança e qualidade dos produtos, bem como de menores custos de transação e preços" [10]. No contexto europeu, a *European Union Agency for Network and Information Security* (ENISA) apoia as organizações europeias de normalização na obtenção de um quadro coerente para normas de cibersegurança na Europa [11].

Depreende-se, assim, que a aplicação de normas, nomeadamente no âmbito da segurança da informação, pode trazer grandes benefícios às empresas e organizações, pois estas consubstanciam a visão e a concordância de intervenientes importantes sobre as melhores

práticas a adotar, os controlos recomendados a implementar, com reflexos positivos na operação, na imagem e na reputação da empresa.

De acordo com Harris, S. [12, p. 20], uma *framework*, ou estrutura, é "utilizada como linha orientadora sobre como construir uma arquitetura que se adeque às necessidades da empresa. A arquitetura de cada empresa será diferente porque as empresas têm diferentes objetivos de negócio, requisitos regulatórios e de segurança, culturas e estruturas organizacionais". Neste contexto, a referida autora indica também que "uma arquitetura corporativa permite que não só se compreenda a empresa de perspetivas diferentes, mas também se entenda como uma mudança num nível irá afetar os outros níveis" [12, p. 20].

O grande benefício das *frameworks* está exatamente na flexibilidade, que permite estabelecer uma arquitetura de segurança adequada à realidade de cada organização, atendendo à base de suporte que possuem, composta por processos e mecanismos estabelecidos para endereçar necessidades de segurança a vários níveis.

A certificação é um conceito com dupla definição, na medida em que pode referir-se a capacidades e conhecimentos adquiridos e comprovados por especialistas em vários domínios da segurança informática ou a um processo de avaliação técnica abrangente dos componentes de segurança de um sistema e da sua conformidade. Para um especialista, uma certificação apresenta-se como um importante indicador de excelência e um compromisso com a qualidade. Já no caso de um sistema, a certificação indica que este "cumpre com os requisitos de segurança do proprietário dos dados. A certificação considera as medidas de segurança tomadas para protegê-lo e o risco residual representado por este" [13, p. 93].

São notórias as vantagens da certificação, quer em termos de carreira para os profissionais que se afirmam através de poderosas credenciais como são as mais bem reputadas certificações no âmbito da cibersegurança, da segurança da informação, ao nível das redes e em outros domínios, quer para as empresas que veem reconhecida a qualidade dos seus sistemas, obtida através de planeamento realizado com base em processos comprovados, de implementações que contemplam controlos adequados e de processos de melhoria contínuos.

Consultada a Lei Portuguesa, o artigo 135º do Código do Procedimento Administrativo [14], estabelece o conceito de regulamentos administrativos como sendo "as normas jurídicas gerais e abstratas que, no exercício de poderes jurídico-administrativos, visem produzir efeitos jurídicos externos". Estes instrumentos legais são "normativos de grau inferior ao ocupado pelas leis, que visam pormenorizá-las e complementá-las com o intuito de viabilizar a sua aplicação ou execução" [15].

Um regulamento da União Europeia "é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países" [16]. O regulamento "tem de ser plenamente respeitado pelos destinatários abrangidos pelo seu âmbito de aplicação. É um ato jurídico que vincula as instituições da UE, os países da UE e os particulares a quem se destina. Sendo imediatamente aplicável como regra em todos os países da UE, o regulamento "não precisa de ser transposto para a legislação nacional, estabelece direitos e obrigações para os particulares que podem,

por conseguinte, invocá-lo diretamente junto dos tribunais nacionais e pode ser utilizado como referência por particulares na sua relação com outros particulares, com os países da UE ou com as autoridades da UE. É aplicável em todos os países da UE a partir da data da sua entrada em vigor (a data que definiu para o efeito ou, na sua falta, 20 dias após a sua publicação no Jornal Oficial). Os seus efeitos jurídicos têm caráter vinculativo simultâneo, automático e uniforme em todas as legislações nacionais" [17].

O trabalho de investigação realizado permitiu identificar um conjunto alargado de instrumentos estabelecidos especificamente para a segurança da informação e das comunicações, tais como:

Normas:

- NP ISO/IEC 27001:2013 [18], ISO/IEC 27002:2013 [19], ISO/IEC 27003:2010 [20], ISO/IEC 27004:2016 [21], ISO/IEC 27005:2011 [22] e NP ISO/IEC 31000:2012 [23], da *International Organization for Standardization* (ISO) e da *International Electrotechnical Commission* (IEC);
- SP 800-61r2, do *National Institute of Standards and Technology* (NIST);

***Frameworks*:**

- *Control Objectives for Information and Related Technology* (COBIT) [24], da *Information Systems Audit and Control Association* (ISACA);
- *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE) [25], da *Carnegie Mellon University* (CMU);
- *Cybersecurity Framework* (CSF) [26], do *National Institute of Standards and Technology* (NIST);

Certificações:

- *Certified Information System Security Professional* (CISSP) [27], *Certified Secure Software Lifecycle Professional* (CSSLP) [28], *Certified Cloud Security Professional* (CCSP) [29] e *Certified Authorization Professional* (CAP) [30], da *International Information System Security Certification Consortium* (ISC)2;
- *Certified Information Systems Auditor* (CISA) [31], *Certified Information Security Manager* (CISM) [32] e *Certified in Risk and Information Systems Control* (CRISC) [33], da ISACA;
- *Security*+ [34], da *Computing Technology Industry Association* (CompTIA);
- *Certified Network Defender* (CND) [35] e *Certified Ethical Hacker* (CEH) [36], da *International Council of Electronic Commerce Consultants* (EC-Council);
- Security Essentials *(GSEC)* [37], Information Security Fundamentals *(GFIS)* [38] e *Certified Enterprise Defender (GCED)* [39], da *System Administration, Networking and Security* (SANS) Institute / *Global Information Assurance Certification* (GIAC);

- Regulamento Geral de Proteção de Dados (RGPD) [9] e a Diretiva sobre Segurança de Redes e Informação[2] [40], ambos da União Europeia.

De entre os recursos relacionados com a temática deste trabalho, destacou-se os supramencionados na medida em que estes são desenvolvidos por entidades referência a nível mundial e cobrem diversos campos de ação, como sejam a identificação de vulnerabilidades, a gestão do risco, o desenvolvimento seguro de *software*, a aplicação de controlos de segurança, a governança e gestão de tecnologias de informação (TI), a resposta a incidentes e a auditoria.

Da análise, constatou-se que as *frameworks* COBIT e NIST CSF são compatíveis na medida em que partilham três aspetos essenciais: ambas têm uma orientação à implementação, ambas fazem referência uma à outra e ambas fornecem uma abordagem holística. Mais concretamente, embora cada *framework* sugira uma metodologia de implementação própria, estas são facilmente mapeadas entre si. O COBIT aborda passo a passo a adoção de boas práticas de governança, enquanto a NIST CSF aponta especificamente para as práticas relacionadas com a cibersegurança. O COBIT refere-se às publicações apropriadas do NIST ao nível do processo, enquanto o NIST refere-se às práticas do COBIT como referências informativas, permitindo um mapeamento mais claro, duplicação reduzida e uma visão mais ampla de um programa de cibersegurança. Um dos princípios do COBIT é "Aplicar uma Abordagem Holística", que assenta num conjunto de habilitadores. A NIST CSF, por outro lado, apresenta também uma abordagem holística para a cibersegurança, pois fornece uma estrutura com cinco funções: Identificar, Proteger, Detetar, Responder e Recuperar, e inclui atividades, resultados desejados e referências aplicáveis.

Quanto às certificações, apurou-se que a certificação CISM é mais direcionada para a gestão e estratégia, nomeadamente questões regulatórias, governança de segurança da informação, análise custo-benefício da mitigação de riscos, gestão do risco e recuperação de incidentes, cobrindo os tópicos técnicos de forma superficial. O CISSP, por seu lado, aborda aspetos táticos das operações de segurança com um nível de aprofundamento muito superior, nomeadamente em oito domínios: segurança e gestão do risco, segurança de ativos, engenharia de segurança, comunicações e segurança de rede, gestão de identidade e acesso, avaliação de segurança e testes, operações de segurança e segurança de desenvolvimento de *software*.

Verificou-se, também, que alguns dos tópicos analisados se sobrepõem por vezes, como é exemplo o caso da norma ISO/IEC 27005:2011, da *framework* OCTAVE e das certificações CAP e CRISC, que lidam todas com a gestão do risco. A CISM mencionada anteriormente também aborda esta temática. Apesar desta coincidência, a escolha por um ou por outro instrumento, ou a possibilidade de se tirar partido de várias fontes de conhecimento, depende sempre do problema a ser resolvido.

[2] 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.

Não sendo praticável, no âmbito deste trabalho, o aprofundamento de todos os instrumentos de segurança referidos, decidiu-se detalhar primeiro a norma ISO/IEC 27001, que é auxiliada por outras normas da mesma família (ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005).

A escolha das normas ISO foi motivada pelo facto de a norma ISO/IEC 27001 ser considerada o padrão *de facto* [41], criado especificamente para gestão da segurança da informação, mais concretamente por "especificar os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação" (SGSI) [18, p. 6].

Não obstante os objetivos dos restantes instrumentos mencionados, que cobrem diversos domínios da segurança da informação, os fundamentos da norma ISO/IEC 27001 e o grande conjunto de ferramentas que os permite concretizar tornaram esta norma não apenas alvo de destaque, mas a primeira escolha para uma análise mais aprofundada. Adicionalmente, a ISO é um organismo com uma reputação e abrangência notáveis, contando com 161 países membros [42], de um total de 195 a nível mundial. Cada país é representado pelo organismo nacional de normalização, que, no caso de Portugal, é o Instituto Português da Qualidade, I.P. (IPQ)[3].

São também alvo de pormenor a *framework* COBIT, por fornecer orientações sobre governança corporativa e gestão de TI e apresentar um modelo de capacidade de processos, a certificação CISA, por ter como um dos principais domínios o processo de auditoria a sistemas de informação, e o RGPD, cuja implementação obrigatória se encontra na ordem do dia, com grandes mudanças nas empresas no que respeita à proteção dos dados pessoais, às atividades de tratamento da informação e às medidas técnicas a implementar para segurança da informação e das comunicações.

Por fim, constatou-se que a norma SP 800 61r2 do NIST, sobre incidentes de segurança informática, cobre todo o ciclo de vida da gestão de incidentes, tendo inclusive uma fase de preparação para a eventualidade de tais ocorrências. A implementação dos requisitos e recomendações desta norma vem facilitar a resposta eficiente e eficaz a incidentes de segurança da informação.

[3] Instituto Português da Qualidade, I.P. (IPQ) - http://www1.ipq.pt/PT/Pages/Homepage.aspx

2.1. NORMA NP ISO/IEC 27001:2013

A norma NP ISO/IEC 27001:2013, traduzida da norma internacional com a mesma nomenclatura, foi desenvolvida pelo comité técnico conjunto formado pela ISO e pela IEC, e publicada pelo IPQ. Trata-se da principal norma da família ISO/IEC 27000:2016 e é o padrão internacional para a gestão da segurança da informação [41], sendo também a única norma internacional passível de certificação e auditoria.

Esta foi a primeira norma portuguesa (NP) de segurança da informação e "constitui um quadro de referência para a gestão de segurança de informação, sendo utilizada como modelo de referência ou como norma certificadora, por um conjunto diversificado de empresas e instituições em todo o mundo" [11].

Uma análise ao cenário de aplicação desta norma em Portugal, a partir dos dados da ISO referentes aos anos de 2015 e de 2016, revela que possuíam certificação ISO/IEC 27001 56 e 96 empresas, respetivamente. Não obstante este elevado crescimento em apenas dois anos, ainda é pouca a importância dada à implementação das melhores práticas de segurança da informação, se considerarmos que no *ranking* europeu de países e respetivo número de entidades certificadas, Portugal ocupava a 22º posição, sendo largamente ultrapassado por países como a Suíça (145), a Irlanda (175), a Hungria (421), a Espanha (752) e os três mais certificados: Itália (1220), Alemanha (1338) e Reino Unido (3367) no ano de 2016 [12].

A norma NP ISO/IEC 27001:2013 tem como objetivo "especificar os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação" (SGSI) [18, p. 6], integrado no sistema global de gestão da empresa, cujo propósito é ajudar a manter seguros os recursos de informação, tais como dados financeiros, dados pessoais de clientes, de fornecedores e de colaboradores, dados partilhados com outras entidades, propriedade intelectual, entre outros.

A sua aplicação numa empresa permite determinar e avaliar os riscos de segurança da informação a que esta está sujeita, implementar procedimentos e mecanismos que permitam preservar a integridade, confidencialidade e disponibilidade da informação, avaliá-los ciclicamente e realizar manutenção e melhorias ao SGSI sempre que necessário. A gestão de incidentes é também contemplada nesta norma. A estrutura organizacional da ISO 27001, nomeadamente as cláusulas 4 a 10 que descrevem os requisitos para cumprimento da norma, e que se apresenta de forma mais detalhada no subcapítulo 2.1.2, indica que o seu funcionamento se enquadra no ciclo de melhoria PDCA: *Plan – Do – Check – Act*.

O ciclo PDCA é um modelo que procura tornar os processos de gestão mais ágeis, claros e objetivos [44]. Segundo Moen e Norman, "o ciclo de quatro etapas para a resolução de problemas inclui o planeamento, a implementação, a verificação dos resultados e a ação. O ciclo PDCA evidencia, também, a prevenção da recorrência de erros ao estabelecer padrões e a constante modificação desses padrões" [45, p. 7].

Esquematicamente, o ciclo PDCA pode ser representado como o círculo na Figura 1:

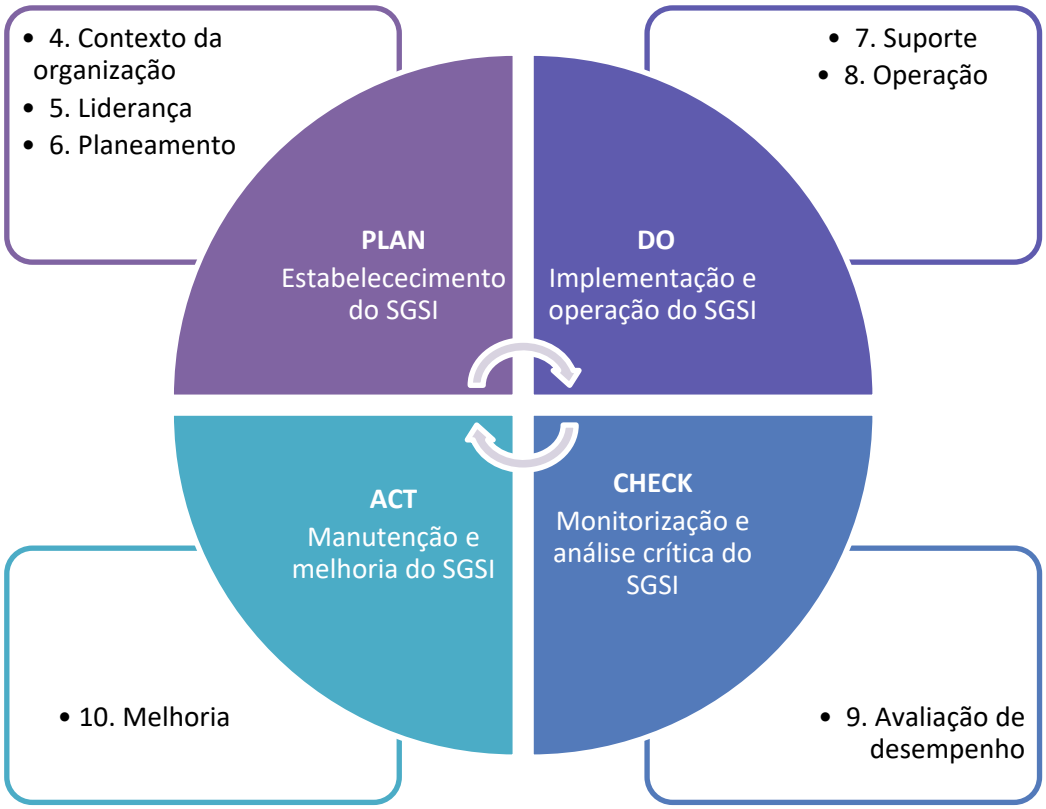


Figura 1 – Ciclo PDCA e cláusulas 4 a 10 da norma ISO/IEC 27001 (adaptado de [46])

No contexto da norma NP ISO/IEC 27001:2013, o ciclo PDCA consiste nas seguintes fases:

PLAN → Fase de planeamento em que é estabelecido o sistema de gestão de segurança de informação, e que inclui os objetivos, os processos e os procedimentos para a gestão do risco, os controlos a aplicar e a documentação a ser produzida.

DO → Fase de implementação e operação do SGSI, com aplicação prática dos controlos, dos processos e dos procedimentos estabelecidos.

CHECK → Fase de avaliação dos indicadores de desempenho dos controlos implementados e confrontação com a política do SGSI. Os resultados da avaliação impõem uma análise crítica e revisão da política, quando aplicável.

ACT → Fase em que são efetuadas ações corretivas e de prevenção aos controlos cujos indicadores de desempenho não apresentaram resultados satisfatórios, com vista à melhoria contínua do SGSI.

2.1.1. Aspetos de Segurança

Na sua introdução, a norma NP ISO/IEC 27001:2013 refere que o SGSI "preserva a confidencialidade, integridade e disponibilidade" [18, p. 5], aspetos de segurança com as seguintes definições no vocabulário da norma:

- **Confidencialidade**: propriedade que a informação não está disponível nem é divulgada a pessoas, entidades ou processos não autorizados;
- **Integridade**: propriedade de exatidão e completude;
- **Disponibilidade**: propriedade de estar acessível e ser utilizável, mediante pedido, por uma entidade autorizada;

Adicionalmente, a norma clarifica que "é importante que o sistema de gestão de segurança da informação faça parte de e esteja integrado com os processos da organização e com a estrutura de gestão global e que a segurança da informação seja considerada na conceção de processos, sistemas de informação e controlos" [18, p. 5]. Desta recomendação podemos inferir que, para além da tríade de requisitos de segurança acima mencionada, podem e devem ser também considerados outros aspetos relevantes para os sistemas da empresa, tais como:

- **Controlo de acesso**: garantia de que o acesso aos ativos é autorizado e restrito com base em requisitos de segurança e de negócio;
- **Não repúdio**: objetivo de segurança que exige que as ações de uma entidade possam ser escrutinadas e atribuídas unicamente a essa entidade. Em caso de violação de segurança ou contestação a uma transação, deverá ser possível analisar os registos de atividade nos sistemas e efetuar o rastreio até à identificação do responsável.
- **Autenticidade**: objetivo de segurança que exige a capacidade de verificar que as entidades são quem dizem ser e que a informação transmitida teve origem numa fonte fidedigna.
- **Conformidade**: objetivo que pretende garantir que a informação é produzida em conformidade com a legislação e/ou outros documentos regulamentares.

Nas empresas circulam ou encontram-se armazenadas informações às quais estão associados níveis de sigilo diferentes. A título de exemplo, uma brochura sobre um curso de formação para conhecimento de todos os colaboradores terá um nível de sigilo distinto de um documento pessoal num processo de recursos humanos. Daqui se deduz que as informações devem, também, ser protegidas de formas distintas.

Para que tal aconteça, é necessário que a informação seja classificada. A classificação permite não só avaliar a informação como também estabelecer critérios de proteção de acordo com essa mesma classificação. Compete à organização definir e estabelecer os níveis de classificação da informação que pretende instituir. De acordo com S. S. Greene, "O sistema de classificação mais comum inclui três níveis: confidencial, sensível e público" [47]:

- **Confidencial**: apenas deve ser disponibilizado para um pequeno subconjunto de colaboradores autorizados. A divulgação não autorizada de informação confidencial causaria danos à empresa.
- **Sensível**: disponível apenas quando há a "necessidade de saber". É, geralmente, disponibilizado a mais colaboradores do que a informação confidencial. A divulgação não autorizada prejudicaria a empresa, especialmente em termos de reputação.
- **Público**: há partilha de informação com o público e a divulgação dessa informação não prejudica a empresa.

A preservação dos três requisitos de segurança principais (confidencialidade, integridade e disponibilidade) é cumprida, segundo a norma NP ISO/IEC 27001:2013, através da aplicação de um processo de gestão de risco. Este é um processo complexo que tem como propósito definir as regras para a identificação de ativos, vulnerabilidades, ameaças, assim como impactos e probabilidade de ocorrência, definindo simultaneamente o nível de risco aceitável. Identificados os riscos, procede-se à implementação do plano de tratamento de risco, sendo os resultados do tratamento devidamente documentados. A norma ISO/IEC 27005:2011, abordada no capítulo 4.1.5, fornece diretrizes sobre a gestão do risco.

2.1.2. Estrutura

A norma NP ISO 27001:2013 carateriza-se por duas componentes, sendo a primeira descrita através de cláusulas que especificam a norma e os requisitos para o seu cumprimento, enquanto a segunda consiste no Anexo A, que contém uma lista com os objetivos de controlo e os controlos a aplicar.

As cláusulas 1 a 3 indicam o objetivo e campo de aplicação da norma, a referência normativa ISO/IEC 27000 que é o documento que contém a visão geral e o vocabulário, e os termos e definições utilizados que apontam para esse documento. Os requisitos para o cumprimento da norma encontram-se nas cláusulas 4 a 10 e é obrigatória a sua inclusão para efeitos de reivindicação de conformidade [18, p. 6]:

4. **Contexto da Organização** – é necessário compreender as questões internas e externa da organização, quais as necessidades e expetativas das partes interessadas, determinar o âmbito do SGSI e estabelecê-lo, implementá-lo, mantê-lo e melhorá-lo de forma contínua de acordo com os requisitos da norma.
5. **Liderança** – a gestão de topo deve demonstrar liderança e compromisso para com o SGSI, estabelecer uma política de segurança da informação e assegurar que são atribuídas e comunicadas as responsabilidades e autoridades para funções que são relevantes para a segurança da informação.
6. **Planeamento** – a organização deve planear ações para abordar riscos e oportunidades, aplicar processos de avaliação e tratamento do risco de segurança mantendo

informação documentada sobre os mesmos, estabelecer objetivos para níveis e funções relevantes determinando o que será feito, que recursos serão necessários, quem será responsável, quando estará concluído e como é que os resultados serão avaliados.

7. **Suporte** – a organização deve proporcionar os recursos necessários ao SGSI, assegurar a competência das pessoas nele envolvidas, consciencializar os colaboradores da política de segurança implementada, determinar a necessidade para as comunicações internas e externas incluindo os processos pelos quais deve ser efetuada e assegurar que a informação documentada é controlada em termos de distribuição, acesso, armazenamento, controlo de versões e eliminação.
8. **Operação** – a organização deve assegurar o controlo operacional, realizar avaliações do risco em intervalos planeados ou quando ocorrem alterações significativas e manter um plano de tratamento do risco.
9. **Avaliação de Desempenho** – a organização deve determinar a monitorização, a medição, a análise e a avaliação a serem realizadas, conduzir auditorias internas para informar da conformidade do SGSI e revê-lo para assegurar a sua contínua aplicabilidade, adequabilidade e eficácia.
10. **Melhoria** – a organização deve reagir a ocorrências de não conformidades e aplicar ações corretivas para que não se repitam e melhorar o SGSI de forma contínua.

O Anexo A, segunda componente da norma, encontra-se organizado da seguinte forma:

- Apresenta 14 secções numeradas sequencialmente de A.5 a A.18;
- Cada secção contém uma ou mais categorias de segurança da informação;
- Cada categoria, por sua vez, contém:
  - Um objetivo de controlo, que é a meta a atingir;
  - Um ou mais controlos, cuja aplicação permitirá alcançar o objetivo de controlo;

Tabela 1 - Secções e controlos de referência do Anexo A

Secção	Controlo de referência	Nº categorias	Nº controlos
A.5	Políticas de segurança de informação	1	2
A.6	Organização de segurança de informação	2	7
A.7	Segurança na gestão de recursos humanos	3	6
A.8	Gestão de ativos	3	10
A.9	Controlo de acesso	4	14
A.10	Criptografia	1	2
A.11	Segurança física e ambiental	2	15

A.12	Segurança de operações	7	14
A.13	Segurança de comunicações	2	7
A.14	Aquisição, desenvolvimento e manutenção de sistemas	3	13
A.15	Relações com fornecedores	2	5
A.16	Gestão de incidentes de segurança da informação	1	7
A.17	Aspetos de segurança da informação na gestão da continuidade do negócio	2	4
A.18	Conformidade	2	8
	TOTAL	**35**	**114**

Na Tabela 1 apresenta-se uma lista das secções e o respetivo número de categorias e controlos do Anexo A. De referir que a empresa ou organização pode conceber os seus próprios controlos caso verifique que a lista do Anexo A não é extensa o suficiente de forma a cobrir as suas necessidades.

2.2. OUTROS PADRÕES E ESTRUTURAS RELACIONADAS

O caráter prático da norma ISO/IEC 27001:2013 justificou a produção, pelas mesmas entidades, de normas auxiliares que, não sendo certificáveis, ajudam, contudo, no planeamento e implementação de um sistema de gestão de segurança da informação. Destas normas destacam-se a ISO/IEC 27002:2013, que inclui uma lista de controlos de segurança, a ISO/IEC 27003:2017 que guia a implementação de um sistema de gestão de segurança da informação (SGSI), a ISO/IEC 27004:2016 sobre a monitorização, medição, análise e avaliação de um SGSI e a ISO/IEC 27005:2011, que incide sobre a gestão do risco da segurança de informação.

No Anexo I apresenta-se uma lista com todas as normas da família ISO/IEC 27000, no entanto, para melhor se compreender as normas auxiliares da ISO/IEC 27001:2013 mais relevantes para este trabalho, optou-se por abordá-las e expor as suas mais-valias no subcapítulo 2.2.1. No seguimento, apresenta-se um conjunto de outros instrumentos também relevantes no contexto da segurança da informação e da auditoria.

A *framework Control Objectives for Information and Related Technology* (COBIT) [49] da ISACA, apresentada no subcapítulo 2.2.2, para além de fornecer uma estrutura corporativa para governança e gestão de TI, contém um modelo de capacidade de processos que se considera importante evidenciar, pois as atividades práticas de segurança da informação consistem normalmente em processos cuja avaliação é importante realizar.

No subcapítulo 2.2.3 é abordada a certificação *Certified Information Systems Auditor* (CISA) [50], que tem como principal foco a auditoria a sistemas de informação. Não sendo uma auditoria específica para o âmbito da segurança, o conhecimento dos seus domínios permite,

no entanto, a identificação de possíveis situações de vulnerabilidade passíveis de melhoria, pelo que se decidiu detalhá-los para melhor compreensão.

O Regulamento Geral de Proteção de Dados (RGPD) [9] é apresentado no subcapítulo 2.2.4, na perspetiva de se compreender o seu propósito e os principais requisitos para o seu cumprimento.

No subcapítulo 2.2.5 apresenta-se a norma NIST SP 800-61r2, criada para "auxiliar as organizações a estabelecer recursos de resposta a incidentes de segurança de informação e de tratamento de incidentes de forma eficiente e eficaz" [58, p. 1].

Por fim, realiza-se uma análise comparativa aos instrumentos analisados, de forma a se compreender onde e como atuam nos planos de uma estrutura organizacional, em que aspetos se destacam e como se podem complementar.

2.2.1. Normas ISO/IEC 27002, 27003, 27004, 27005, 27035 e 31000

A norma ISO/IEC 27002:2013 foi projetada para ser "uma referência na seleção de controlos dentro do processo de implementação de um sistema de gestão da segurança da informação (SGSI), baseado na ISO/IEC 27001" [19], pois define as orientações e os princípios para a análise dos requisitos de cada um dos controlos estabelecidos na ISO/IEC 27001:2013. Trata-se, no fundo, de um código de práticas que inclui um extenso conjunto de controlos que indicam a forma de atuação para que os objetivos definidos nas políticas possam ser atingidos.

Os controlos devem estar enquadrados com as decisões da empresa, e estas fundamentadas no nível de risco que a empresa defina como aceitável, nas opções para o seu tratamento e na gestão de risco realizada. Para estar em conformidade legal é fundamental a definição de controlos para a proteção de dados pessoais, a salvaguarda dos registos da empresa e o zelo pelos direitos de propriedade intelectual.

Das práticas de segurança da informação fazem parte a documentação que contém a política de segurança, a esfera de responsabilidades, e três tipos de gestão: a gestão de vulnerabilidades técnicas, a gestão de incidentes de segurança e a gestão da continuidade do negócio, que contempla as melhorias a realizar.

A estrutura da norma ISO/IEC 27002:2013 coincide com a estrutura do Anexo A da NP ISO/IEC 27001:2013 apresentada anteriormente na Tabela 1. No Anexo II é apresentado um quadro-resumo que inclui os objetivos de controlo.

A ISO/IEC 27003:2010 é a norma que disponibiliza diretrizes para a implementação de um SGSI. O âmbito desta norma é claro ao indicar que esta "descreve o processo de especificação e *design* do SGSI desde o início até a produção de planos de implementação" [20, p. 7]. A mais recente revisão desta norma veio alinhá-la com a estrutura da ISO/IEC 27001:2013 no que respeita às cláusulas 4 a 10, indicando para cada cláusula a atividade requerida em conjunto

com a explicação e orientação para a implementação. Um anexo com a definição da estrutura da política complementa as orientações definidas.

As métricas de segurança a aplicar a um SGSI constam da norma ISO/IEC 27004:2016. Esta norma tem como propósito "ajudar as organizações na avaliação da eficácia e da eficiência de um SGSI de modo a que este cumpra os requisitos da cláusula 9.1 da ISO/IEC 27001:2013" [21, p. 7]. Para tal, esta norma "estabelece:

- a monitorização e medição do desempenho da segurança da informação;
- a monitorização e medição da eficácia de um SGSI, incluindo os seus processos e controlos;
- a análise e avaliação dos resultados da monitorização e da medição" [21, p. 7].

A aplicação deste padrão permite obter informações necessárias para a gestão e melhoria do SGSI.

A norma ISO/IEC 27005:2011 "fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a ISO/IEC 27001" [22, p. 6]. Este tipo de gestão consiste num processo contínuo de observação do contexto, de identificação e avaliação dos riscos e do seu tratamento. Esta norma não providencia um método específico e indica que "cabe à organização definir a sua abordagem ao processo de riscos" [22, p. 6], que poderá ser feita de acordo com o âmbito do SGSI, o contexto da gestão do risco ou o setor de atividade económica.

Para lidar com a gestão de incidentes, a ISO/IEC criou a norma 27035:2016, que se encontra dividida em duas partes: a primeira parte introduz os princípios de gestão de incidentes [51], enquanto a segunda parte apresenta diretrizes para planear e preparar a resposta a incidentes [52]. A necessidade desta norma decorre de os controlos de segurança da informação poderem falhar de alguma forma. Entre possíveis problemas, os controlos podem ser comprometidos através de *malware* ou por *hackers*, o seu funcionamento pode não ser o adequado verificando-se lentidão na deteção de anomalias ou a implementação do controlo pode não estar concluída por falta de dados resultante da análise de riscos. Por estes e outros motivos, os incidentes de segurança da informação podem ocorrer mesmo em empresas que impõem políticas restritas de segurança de informação.

De realçar que "a gestão eficaz de incidentes envolve controlos de deteção e correção definidos para reconhecer e responder a eventos e incidentes, minimizar os impactos adversos, recolher provas e, em devido tempo, 'aprender as lições' para melhoria dos controlos preventivos ou outros tratamentos de risco" [53, Par. 2].

Fora da família ISO/IEC 27000, mas igualmente sobre a Gestão do Risco, a norma NP ISO 31000:2012 "fornece os princípios e as linhas de orientação para a gestão de qualquer tipo de risco de modo sistemático, transparente e credível, qualquer que seja o âmbito e o contexto" [23, p. 6]. A inclusão do estudo desta norma prendeu-se com a indicação na NP ISO/IEC

27001:2013 de que "o processo de avaliação e tratamento do risco de segurança da informação nesta norma está alinhado com os princípios e diretrizes genéricas disponibilizadas na NP ISO 31000:2012" [18, p. 9].

2.2.2. COBIT – *Control Objectives for Information and Related Technology*

O COBIT, atualmente na versão 5, é um modelo corporativo para a governança e gestão de tecnologia de informação (TI) desenvolvido pela *Information Systems Audit and Control Association* (ISACA), que "ajuda as organizações a criar valor através da TI mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos" [49, p. 15].

Através de um esquema prático em forma de cascata, este é um modelo holístico que permite traduzir os objetivos corporativos de alto nível em objetivos de TI, específicos e geríveis, mapeando-os em práticas e processos também estes específicos. Para apoiar a implementação de um sistema abrangente de governança e gestão de TI, o COBIT 5 estabelece um conjunto de habilitadores, que mais não são do que fatores que influenciam o seu funcionamento. São sete as categorias de habilitadores do COBIT 5, como se pode observar na ***Figura 2***:

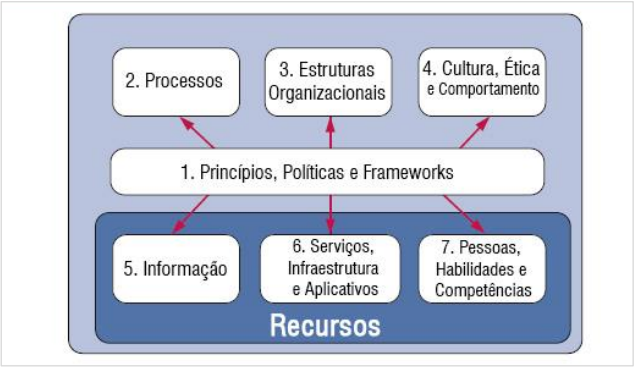


Figura 2 – Habilitadores do COBIT 5 **[49, p. 29]**

Orientados pela cascata de objetivos, apresentada na ***Figura 3***, os objetivos de TI nos níveis superiores definem os objetivos que os diferentes habilitadores devem alcançar. Cada habilitador tem diversas metas, criando-se valor quando estas são atingidas. Tal é verificado através da métrica associada à meta a atingir. As metas são a última etapa da cascata de objetivos do COBIT 5.

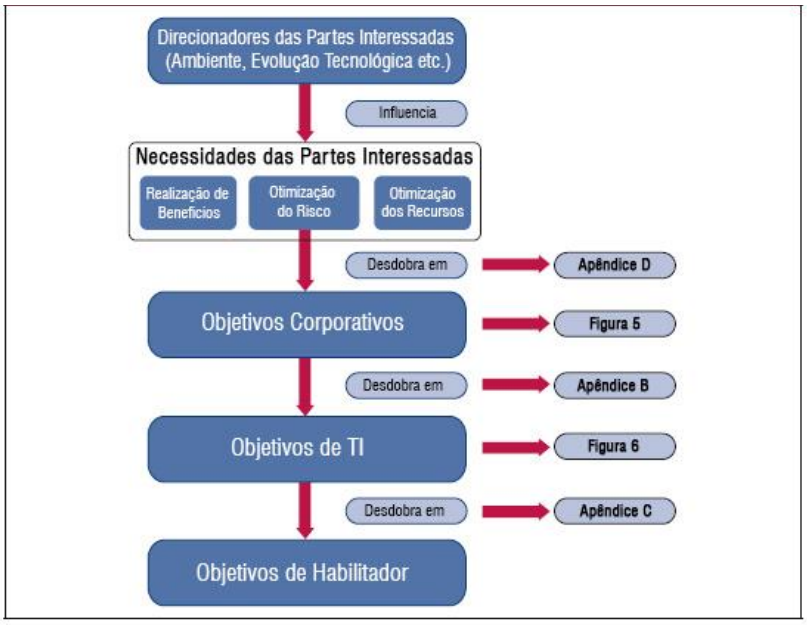


Figura 3 – Cascata de objetivos do COBIT 5 **[49, p. 20]**

A distinção entre governança e gestão é claramente identificada no COBIT 5, pois estas requerem estruturas organizacionais diferentes, atendem a propósitos diferentes e abrangem diversos tipos de atividade. O COBIT 5 inclui um modelo de referência de processo, apresentado no Anexo IV [49, p. 35], que divide os processos de governança e de gestão de TI:

- A **governança** contém cinco processos, sendo que para cada processo são definidas práticas para Avaliar, Dirigir e Monitorizar (*Evaluate, Direct and Monitor - EDM*).

- A **gestão** contém quatro domínios, em consonância com as áreas responsáveis pelo planeamento, construção, execução e monitorização (*Plan, Build, Run and Monitor - PBRM*), e oferece cobertura de tecnologias de informação de ponta a ponta. Os nomes dos domínios são descritos através de verbos, congruentes com as designações das áreas principais:

    - Alinhar, Planear e Organizar (*Align, Plan and Organise – APO*)
    - Construir, Adquirir e Implementar (*Build, Acquire and Implement – BAI*)
    - Entregar, Serviço e Suporte (*Deliver, Service and Support - DSS*)
    - Monitorizar, Avaliar e Analisar (*Monitor, Evaluate and Assess – MEA*)

A implementação do COBIT 5 baseia-se em três componentes do ciclo de vida apresentado na ***Figura 4*** [49, p. 39]:

1. **O ciclo de vida de melhoria contínua**, que indica o seu cariz iterativo, não sendo, portanto, um projeto único e isolado;
2. **A capacitação de mudança**, numa abordagem a aspetos comportamentais e culturais;

3. **A gestão do programa**;

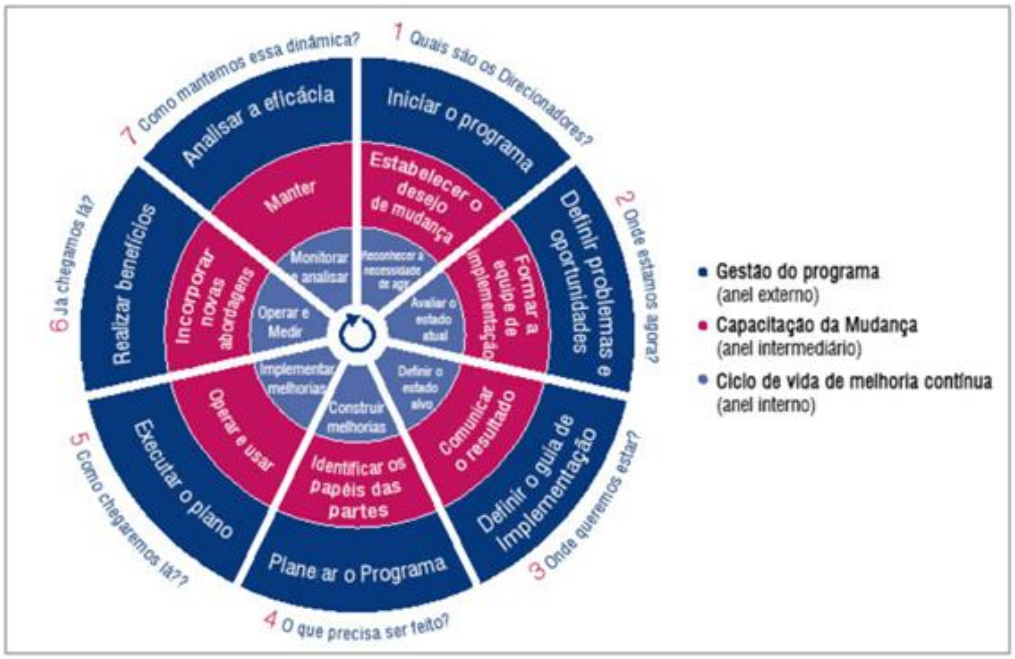


Figura 4 – Ciclo de vida da implementação do COBIT 5 **[49, p. 39]**

O ciclo de vida decorre ao longo de sete fases, que se resumem em seguida:

Na 1ª fase é reconhecida e aceite a necessidade de uma implementação. São identificados os atuais pontos fracos e é desencadeado o desejo de mudança nos níveis de gestão executiva.

A 2ª fase foca na definição do objetivo da implementação, usando o mapeamento dos objetivos corporativos do COBIT em objetivos de TI e nos respetivos processos de TI, considerando também de que forma os cenários de risco podem destacar os processos em que a empresa se deve concentrar. É realizada uma avaliação do estado atual, sendo os problemas ou as deficiências identificadas através de uma avaliação da capacidade do processo.

O **Modelo de Capacidade de Processo do COBIT 5** indica que um processo pode atingir seis níveis de capacidade [49, p. 46]:

Tabela 2 - Níveis de Capacidade de Processo do COBIT 5

Nível	Capacidade	Descrição	Contexto
0	Processo Incompleto	O processo não foi implementado ou não atingiu o objetivo.	Conhecimento Individual
1	Processo Executado	(um atributo) - O processo implementado atinge o objetivo.	
2	Processo Gerido	(dois atributos) - O processo executado, nível 1, é implementado de forma administrativa (planeado, monitorizado e ajustado) e os produtos do trabalho	

		são adequadamente estabelecidos, controlados e mantidos.	
3	Processo Estabelecido	(dois atributos) - O processo gerido, nível 2, é implementado utilizando um processo definido capaz de atingir os resultados.	Conhecimento Corporativo
4	Processo Previsível	(dois atributos) - O processo estabelecido, nível 3, opera agora dentro dos limites definidos para produzir os resultados.	
5	Processo Otimizado	(dois atributos) - O processo previsível, nível 4, é continuamente melhorado visando atingir os objetivos corporativos pertinentes, atuais ou previstos.	

Atingir a capacidade de processo nível 1 "exige que o atributo "desempenho do processo" seja amplamente atingido" [49, p. 44]. Este é um nível muito importante, essencial para que níveis superiores possam ser alcançados. A medição da capacidade de processo baseia-se nos nove atributos, apresentados na ***Figura 5*** [54, p. 10]:

Nível 1: **Executado** – Atributo: desempenho do processo;

Nível 2: **Gerido** – Atributos: gestão de desempenho e gestão de produto do trabalho;

Nível 3: **Estabelecido** – Atributos: definição do processo e implementação do processo;

Nível 4: Previsível – Atributos: gestão do processo e controlo do processo;

Nível 5: **Otimizado** – Atributos: inovação do processo e otimização do processo

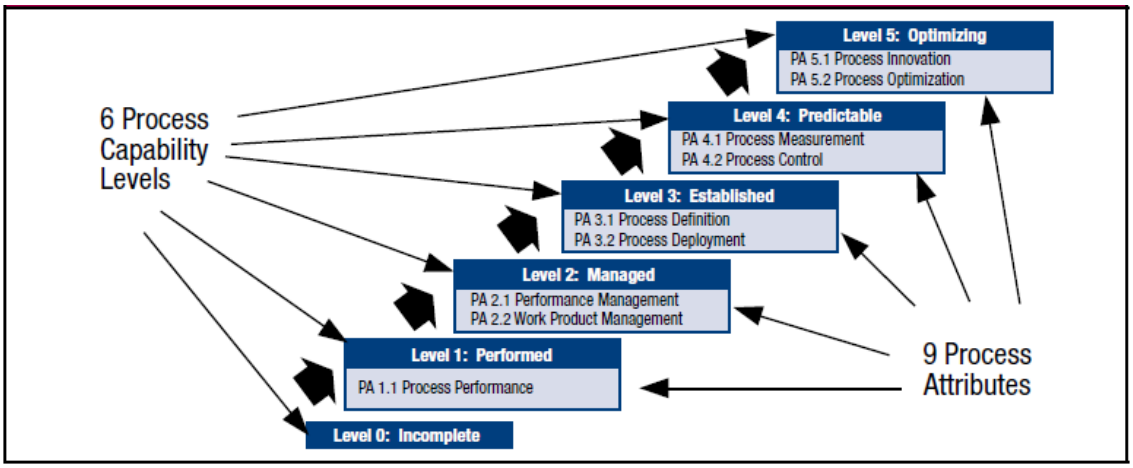


Figura 5 – Atributos de processo do COBIT 5 **[54, p. 10]**

O COBIT 5 estabelece que, para avaliar se um processo atinge os objetivos, ou seja, se atinge a capacidade nível 1, deve-se analisar os resultados do processo de acordo com a descrição na

Tabela 2 e classificar o grau de consecução utilizando, por exemplo, a escala de classificação da norma ISO/IEC 15504[4] [49, p. 48]:

- **N (Não atingido)** – Há pouca ou nenhuma evidência do atingimento de atributos definidos no processo avaliado. (0 a 15 por cento)
- **P (Parcialmente atingido)** – Há pouca evidência da abordagem e baixo atingimento do atributo definido no processo avaliado. Alguns aspetos do atingimento do atributo podem ser imprevisíveis (15 a 50 por cento).
- **L (Amplamente atingido)** – Há evidência da abordagem sistemática e atingimento significativo do atributo definido no processo avaliado. Alguns pontos fracos referentes a este atributo podem existir no processo avaliado (50 a 85 por cento).
- **F (Plenamente atingido)** - Há evidência da abordagem completa e sistemática e pleno atingimento do atributo definido no processo avaliado. Não existe nenhum ponto fraco significativo referente a este atributo no processo avaliado (85 a 100 por cento).

Na 3ª fase uma meta de melhoria de um processo é definida e analisada detalhadamente, alavancando a orientação do COBIT no sentido de identificar falhas e possíveis soluções.

A 4ª fase assenta no planeamento de soluções práticas, que são implementadas na 5ª fase. Podem ser definidas medições e monitorização através das metas e indicadores para garantir que o alinhamento da organização é atingido e mantido e que o desempenho pode ser medido.

A 6ª fase concentra-se na operação e na monitorização dos benefícios esperados. Durante a 7ª fase, o sucesso da iniciativa é analisado globalmente. Novos requisitos para a governança ou gestão de TI da organização são identificados e a necessidade de melhoria contínua é reforçada, dando início a um novo ciclo de vida. [49, pp. 39–40]

O sucesso da implementação do COBIT ou de iniciativas de melhoria passa pela criação de um ambiente adequado, no qual se deve verificar o apoio e orientação das principais partes interessadas, tais como a Administração e as Direções de Serviços, de modo a garantir a sintonia e o compromisso com o programa.

2.2.3. CISA – *Certified Information Systems Auditor*

CISA é uma certificação disponibilizada pela ISACA, reconhecida internacionalmente e destinada a profissionais e auditores da área de segurança da informação. Os conteúdos teóricos e práticos desta certificação fornecem ao auditor as competências para identificar

[4] A norma ISO/IEC 15504:2003, revista pela ISO/IEC 33002:2015, define os requisitos para a realização da avaliação de processo para utilização na melhoria dos processos e determinação da capacidade.

problemas críticos e aplicar práticas no sentido de aumentar e consolidar a confiança nos sistemas de informação. A CISA abrange cinco domínios:

1. O **Processo de Auditoria de Sistemas de Informação** aborda a estratégia de auditoria baseada no risco, o planeamento e a realização de auditorias, a realização de autoavaliações de controlo e a comunicação de resultados.
2. A **Governança e Gestão de Tecnologias de Informação** (TI) consiste na avaliação da estratégia, da estrutura de governança e de organização das TI, na gestão de ativos, recursos humanos, políticas, normas e procedimentos. Considera também a avaliação de práticas de gestão de risco, de gestão de TI, de controlos e de indicadores de desempenho.
3. **Aquisição, Desenvolvimento e Implementação de Sistemas de Informação** é o domínio que contém a avaliação de investimentos propostos, de seleção de fornecedores e de processos de gestão de contratos. Inclui, igualmente, a avaliação da gestão de projetos até à fase de implementação.
4. **Operações, Manutenção e Gestão de Serviços de Sistemas de Informação** constituem o domínio que trata a gestão de serviços de TI, nomeadamente a realização de avaliações aos sistemas de informação, operações, manutenção, gestão de problemas e incidentes, continuidade e resiliência, e testes de recuperação de desastres.
5. A **Proteção de Ativos de Informação**, no quinto domínio, tem como conteúdos a avaliação da segurança da informação, da privacidade, de controlos físicos e ambientais, de controlos de segurança lógicos e do sistema, da classificação de dados e salvaguarda de ativos de informação e de programas de segurança da informação. [55]

À semelhança do COBIT, a CISA é orientada para modelos aplicados à tecnologia da informação, no entanto não é uma certificação específica para a segurança da informação.

2.2.4. RGPD – Regulamento Geral da Proteção de Dados

O Regulamento Geral de Proteção de Dados da União Europeia [9], estabelecido em 2016, fornece aos cidadãos uma ampla gama de direitos e limita a capacidade das empresas de processar legalmente dados pessoais da forma como regularmente o faziam até então. Estes novos direitos causam grande impacto nos modelos de operação das empresas, que têm de os ajustar para contemplar a privacidade individual.

As elevadas coimas a aplicar em caso de incumprimento obrigam a um esforço proactivo de conformidade, sendo as principais áreas foco de atuação a informação a disponibilizar aos titulares dos dados, a obtenção do seu consentimento para o tratamento dos dados incluindo dados sensíveis, o exercício dos seus direitos e a documentação e registo das atividades de tratamento. São igualmente fundamentais a proteção de dados desde a conceção dos sistemas, a segurança durante o tratamento, a avaliação do risco e a notificação de violações de segurança. [9, pp. 2–3]

A figura do encarregado de proteção de dados, obrigatória no caso de entidades públicas, tem como principal incumbência "garantir que a organização cumpre todas as obrigações legais desde o início da aplicação do regulamento" [9, p. 3].

2.2.5. NIST SP 800-61r2 – *Computer Security Incident Handling Guide*

A realização de avaliações de risco, como preconizam as normas ISO/IEC 27005:2011 e ISO/IEC 31000:2012, permite identificar medidas de prevenção a implementar com o objetivo de reduzir o número de incidentes de segurança. No entanto, realisticamente, não é possível evitá-los totalmente. A provável ocorrência de incidentes de segurança exige às empresas capacidade para rapidamente os detetar através de análise aos eventos de segurança, minimizar o seu impacto, atenuar os pontos fracos explorados e restaurar os serviços ao seu normal funcionamento.

Para dar resposta a esta realidade, o *National Institute of Standards and Technology* (NIST) criou a *special publication* SP 800-61r2 [56], para "auxiliar as organizações a estabelecer recursos de resposta a incidentes de segurança de informação e de tratamento de incidentes de forma eficiente e eficaz" [56, p. 1]. Para o NIST, "entender as ameaças e identificar os ataques nas fases iniciais é fundamental para evitar comprometimentos subsequentes e a partilha proativa de informações entre as organizações em relação a sinais de ocorrência desses ataques é uma maneira cada vez mais eficaz de identificá-los" [56, p. 1].

Clarificando a terminologia, para o NIST "um evento é qualquer ocorrência observável num sistema ou rede" [56, p. 6], por exemplo um servidor que recebe um pedido para uma página *Web*, um utilizador que envia um *e-mail* ou uma *firewall* que bloqueia uma tentativa de ligação. A norma considera eventos adversos os "eventos com consequências negativas" [56, p. 6], tais como falhas do sistema, inundações de pacotes, acesso não autorizado a dados confidenciais ou a execução de *malware* para destruição de dados. Já um incidente de segurança informática "é uma violação ou uma ameaça iminente de violação de políticas de segurança de informação, de políticas de utilização aceitáveis ou de práticas de segurança padrão" [56, p. 6].

Nesta norma, o NIST apresenta o ciclo de vida da gestão de incidentes, aqui representado na ***Figura 6***:

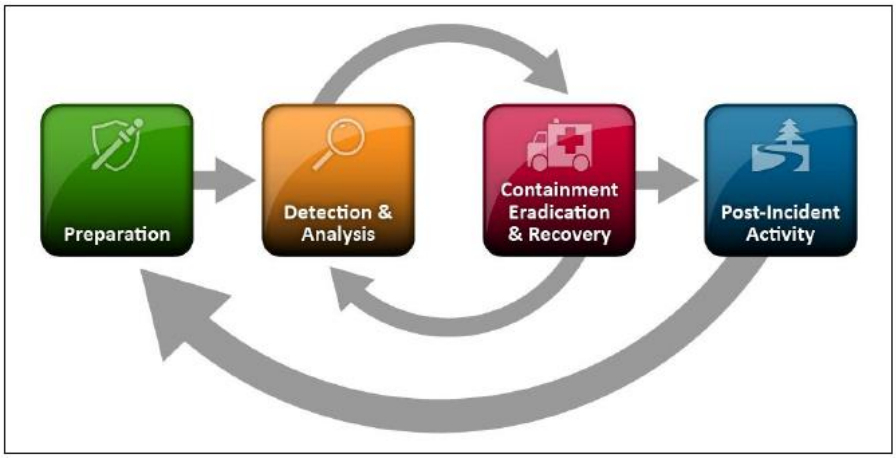


Figura 6 – Ciclo de vida da resposta a incidentes **[56, p. 21]**

A fase de preparação consiste em "não apenas estabelecer uma capacidade de resposta a incidentes, de modo a que a organização esteja pronta para responder a incidentes, mas também evitar incidentes, garantindo que os sistemas, as redes e as aplicações estão suficientemente seguras" [56, p. 21]. Entre as tarefas de preparação estão a adoção de mecanismos de comunicação e coordenação redundantes caso algum venha a sofrer alguma anomalia, a definição de políticas e procedimentos de resposta a incidentes, a formação aos especialistas de segurança, a disponibilização de *hardware* e *software* adequado à análise de eventos (e.g. media amovíveis, *sniffers*, aplicações forenses), *software* para mitigação de incidentes (e.g. imagens dos sistemas para fins de recuperação) e qualquer outro recurso que possa ser útil para lidar de forma eficiente e rápida com um incidente de segurança [56, pp. 22–23].

Na segunda fase são detetados e analisados eventos de segurança com o objetivo de determinar se serão considerados incidentes e, caso o sejam, quais os vetores de ataque associados. Para que a deteção seja possível, é necessário que a empresa disponha de sistemas com automatismos capazes de registar os eventos e de capacidade investigativa para os analisar em tempo útil. Entre os vetores de ataque mais comuns encontram-se os ataques a partir de dispositivos amovíveis, os ataques por força bruta, a exploração de *scripts* em aplicações *Web*, as mensagens de *e-mail* como veículo para *links* e anexos maliciosos ou a personificação através de *access points* corruptos [56, p. 25].

Identificado um incidente, inicia-se a fase de contenção em que a *Computer Emergency Response Team* (CERT), equipa especializada e treinada para monitorizar, identificar e responder a incidentes de segurança, inicia a interação com os sistemas afetados e tenta evitar a propagação dos danos resultantes do incidente. "Uma parte essencial da contenção é a tomada de decisão" [56, p. 35] na medida em que pode envolver o isolamento do sistema da rede, o isolamento do tráfego, o corte de energia ou outros controlos, de acordo com o alcance e gravidade do incidente.

Contido o incidente, isto é, evitada a propagação a outros sistemas, surge a etapa de erradicação ou mitigação. "Durante a erradicação, é importante identificar todos os *hosts* afetados dentro da organização para que estes possam ser remediados" [56, p. 37]. A

erradicação requer também o conhecimento da causa do incidente para que seja possível restaurar o sistema ao estado normal de funcionamento. Determinar a causa de um incidente é fundamental para que não se dê o caso do sistema se manter comprometido ou vir a sofrer um novo incidente pelo mesmo motivo.

A recuperação de um sistema dá-se com a reposição ao seu estado normal de funcionamento, ou seja, ao ambiente de produção, devendo este ser monitorizado para garantir que a erradicação da ameaça foi realmente efetuada com sucesso. "A recuperação pode envolver ações como restaurar sistemas a partir de *backups* válidos, reconstruir sistemas de raiz, substituir ficheiros comprometidos por versões limpas, instalar *patches*, alterar palavras-passe e reforçar a segurança do perímetro de rede (e.g. regras na *firewall*)" [56, p. 37].

Desde a fase inicial de deteção de um incidente até a fase de recuperação do sistema ocorre uma outra fase em paralelo: a fase de reporte. O reporte de um incidente deve ter início assim que seja detetada atividade maliciosa num sistema e deve ser feito em duas vertentes: o reporte técnico e o reporte não-técnico.

Detalhes técnicos devem ser reportados pela CERT assim que a equipa inicia os procedimentos para lidar com o incidente. A norma é clara ao indicar que "todas as etapas desde o momento em que o incidente foi detetado até à sua resolução final devem ser documentadas e registadas com data e hora. Todos os documentos relacionados com o incidente devem ser datados e assinados pelos especialistas" [56, p. 31].

Um sistema de rastreio de problemas deve ser utilizado para registar e acompanhar o estado dos incidentes e outras informações relevantes. A norma indica que "este sistema deve conter informação sobre:

- O estado atual do incidente (e.g. novo, em curso, encaminhado para investigação, resolvido etc.)
- Um resumo do incidente
- Indicadores relacionados com o incidente
- Outros incidentes relacionados com este incidente
- Ações de todos os especialistas sobre este incidente
- Cadeia de responsabilidades, se aplicável
- Avaliações de impacto relacionadas com o incidente
- Informações de contato com outras partes envolvidas (e.g., proprietários do sistema, administradores do sistema)
- Uma lista de evidências recolhidas durante a investigação ao incidente
- Comentários dos especialistas da equipa
- Etapas seguintes a cumprir (e.g., reconfigurar um *host*, atualizar uma aplicação)" [56, p. 31].

Simultaneamente, quando se trate de incidentes graves, devem ser estabelecidos e mantidos canais de comunicação adequados com a Administração da empresa e com as autoridades competentes no sentido de notificá-las e mantê-las atualizadas sobre o desenvolvimento das ações. Reportes formais devem ser produzidos quando a situação já se encontra controlada e os sistemas estão prestes a reentrar em produção.

As atividades pós-incidente constituem a fase de maior potencial para a CERT, por poder resultar em aprendizagem e melhorias nos procedimentos e na postura adotada até então. Uma reunião entre as partes envolvidas deve ter lugar, onde uma série de questões deve ser respondida, como por exemplo:

- Exatamente o que aconteceu e em que momentos?
- Quão bom foi o desempenho da equipa técnica e da Administração ao lidar com o incidente?
- Os procedimentos documentados foram seguidos? Eles foram adequados?
- Que informações foram necessárias mais cedo?
- Foram tomadas medidas ou realizadas ações que possam ter impossibilitado a recuperação?
- O que é que a equipa técnica e a gestão farão de maneira diferente na próxima vez que ocorrer um incidente semelhante?
- Como é que a partilha de informações com outras organizações pode ser melhorada?
- Que ações corretivas podem evitar incidentes semelhantes no futuro?
- Que precursores ou indicadores devem ser observados no futuro para detetar incidentes semelhantes?
- Que ferramentas ou recursos adicionais são necessários para detetar, analisar e mitigar incidentes futuros? [56, p. 38]

Nesta etapa é elaborado o relatório final a ser apresentado à Administração, que deve conter as respostas e as conclusões.

2.3. ANÁLISE COMPARATIVA

As normas e modelos analisados foram concebidos para trazer benefícios às empresas, independentemente da sua natureza ou dimensão. A ***Figura 7*** [57, p. 13] apresenta a pirâmide com os planos da estrutura organizacional de uma empresa mapeados em relação ao gráfico de posicionamento da *framework* COBIT, da norma ISO 27001 e das práticas internas:

- **Plano estratégico** – plano superior onde residem as decisões sobre a estratégia da empresa.

- **Plano tático** – plano intermédio que inclui o controlo de processos e a sua execução, sendo esta partilhada com o nível operacional;

- **Plano operacional** – é a base da pirâmide, onde se conjuga a execução dos processos com as instruções específicas do trabalho, isto é, com as práticas internas.

Os quatro níveis do gráfico integram dois eixos verticais de sentidos opostos. O primeiro eixo, "O Quê", estabelece o posicionamento de cada um dos instrumentos enquanto o eixo "Como" indica a forma de aplicação. O eixo horizontal estabelece o âmbito de cobertura dos instrumentos.

Assim, o COBIT atua entre o plano estratégico e o plano tático, que corresponde às áreas de governança e de gestão da *framework*, tem aplicação "top-down" e cobre todas as áreas da empresa.

A ISO 27001, por seu lado, tem um posicionamento mais alargado, pois toca nos três planos da estrutura organizacional, com aplicação também "top-down", no entanto, por ser uma norma para "especificar os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação" [18, p. 6], o seu âmbito não é abrangente a todas as áreas da empresa.

Já as práticas internas situam-se no nível inferior do gráfico, pois são de natureza exclusivamente operacional e cobrem todas as áreas da empresa.

Figura 7 – Modelo de estrutura organizacional (adaptado de [57, p. 13])

A implementação de um sistema de gestão de segurança da informação indica o evidente compromisso com a segurança, pelo que a nível estratégico o SGSI resultante da implementação da norma NP ISO/IEC 27001:2013 deverá alinhar-se com os objetivos da empresa. O esquema apresentado indica claramente no eixo vertical que, com a aplicação desta norma, a empresa é capaz de demonstrar a estratégia adotada, o controlo de processos e a sua execução.

Para o alinhamento da norma NP ISO/IEC 27001:2013 com os objetivos da empresa, é fundamental que haja uma visão de topo sobre o esquema organizacional, a direção dos objetivos corporativos e as necessidades da empresa. O COBIT, situado entre o plano estratégico e o plano tático, é um modelo corporativo para governança e gestão de tecnologias de informação, estruturado para que seja possível governar considerando a informação e as tecnologias que a suportam. Ao incluir um modelo de capacidade de processos, o COBIT 5 proporciona "meios para medir o desempenho de qualquer um dos processos de governança ou de gestão e permite a identificação das áreas que precisam de ser melhoradas" [49, p. 43].

Segundo a ISACA [49, p. 64], no que respeita a pontos comuns, "as seguintes áreas e domínios do COBIT 5 são cobertas pela família ISO/IEC 27000:

- Processos relativos à segurança e riscos dos domínios:
    - Avaliar, Dirigir e Monitorizar (*Evaluate, Direct and Monitor - EDM*);
    - Alinhar, Planear e Organizar (*Align, Plan and Organise – APO*);
    - Entregar, Serviços e Suporte (*Deliver, Service and Support - DSS*)
- Diversas atividades de segurança dentro dos processos noutros domínios;
- Atividades de monitorização e avaliação a partir do domínio Monitorizar, Avaliar e Analisar (*Monitor, Evaluate and Assess – MEA*)"

Outro aspeto comum relaciona-se com a avaliação de desempenho da segurança da informação e a eficácia do SGSI. A norma NP ISO/IEC 27001:2013 indica que "a organização deve determinar: o que necessita ser monitorizado e medido, incluindo os processos e controlos de segurança da informação; os métodos para monitorizar, medir, analisar e avaliar, conforme aplicável, para garantir resultados válidos; quando deve ser realizada a monitorização e medição; quem deve monitorizar e medir; quando os resultados da monitorização e medição devem ser analisados e avaliados; quem deve analisar e avaliar estes resultados" [18, p. 13]. No COBIT, "para cada habilitador um conjunto específico de metas relevantes pode ser definido para apoiar os objetivos de TI" [49, p. 20].

No entanto, constatam-se também algumas diferenças, pois enquanto a norma NP ISO/IEC 27001:2013 segue as 4 fases do ciclo PDCA – *Plan, Do, Check, Act* –, o COBIT estabelece quatro domínios para a gestão, cujo mapeamento direto com o PDCA não se verifica. Por exemplo, a fase *Check* do PDCA não tem correspondência direta com o domínio DSS - *Deliver, Service and Support*. Uma outra diferença encontra-se no modelo de capacidade de processos do COBIT, que não encontra correspondência na norma NP ISO/IEC 27001:2013.

Não obstante as diferenças entre a norma NP ISO/IEC 27001:2013 e o COBIT, é possível a conjugação das suas mais-valias. Um ponto importante e central no COBIT é o foco nos processos de TI. Estes são desenvolvidos num modelo que utiliza o conceito "*control objectives*" (objetivos de controlo), termo este familiar na implementação de um SGSI.

Na medida em que a norma NP ISO/IEC 27001:2013 contempla a gestão de risco, com suporte na norma auxiliar ISO/IEC 27005:2011, esta componente permite a uma empresa desencadear um processo de autoconhecimento mais aprofundado, assim como dos sistemas de informação que dispõe, dos problemas que ocorrem e da proteção aplicada, de modo a assegurar a disponibilidade de dados e recursos e garantir a sua integridade e continuidade.

É aspeto de destaque na norma NP ISO/IEC 27001:2013 o foco na segurança da informação. A implementação de um SGSI tem como expetativa a redução da probabilidade de ocorrência de

falhas de segurança, a garantia de melhor salvaguarda dos ativos tecnológicos e da informação, a conformidade com os requisitos legais que lhe são aplicáveis e a afirmação da reputação da empresa como credível e de confiança perante os clientes, fornecedores, parceiros e outras entidades. Também financeiramente pode a empresa reduzir os custos associados à ocorrência de incidentes.

O COBIT 5, apesar de contemplar a gestão de risco no domínio APO - Alinhar, Planear e Organizar [49, p. 62], apresenta-se desenhado para lidar com questões de gestão da informação de uma forma mais generalizada, enquanto a norma NP ISO/IEC 27001:2013 é integralmente fundamentada na segurança da informação.

Comparativamente à norma NP ISO/IEC 27001:2013, a certificação CISA, tal como o COBIT, está mais focada nos aspetos relacionados com os sistemas de informação. Por exemplo, a CISA não oferece muitos pormenores relacionados com Segurança de recursos humanos (secção A.7 da norma), ou com a Segurança física e ambiental (secção A.11 da norma). Por outro lado, fornece informações sobre práticas relacionadas com a secção A.6 (Organização de segurança da informação), a secção A.8 (Gestão de ativos) no domínio 5, a secção A.12 (Segurança de operações) no domínio 4 e a secção A.14 (Aquisição, desenvolvimento e manutenção de sistemas) no domínio 3 [50]. Estes pontos comuns indicam a possibilidade das práticas CISA poderem complementar a norma NP ISO/IEC 27001:2013.

Já o Regulamento Geral de Proteção de Dados (RGPD) relaciona-se com a norma NP ISO/IEC 27001:2013 na medida em que a conformidade com este regulamento exige às empresas um conjunto de requisitos que são comuns à norma. A implementação de um sistema de gestão de segurança de informação numa empresa dará resposta à maioria dos requisitos do regulamento, sendo de destacar os seguintes:

- **gestão de ativos** – o RGPD exige às empresas que identifiquem os dados recolhidos, os meios de recolha, a localização de armazenamento, os períodos de conservação e quem acede aos mesmos. A NP ISO/IEC 27001:2013, por seu lado, indica que devem ser identificados os ativos da organização e definidas as responsabilidades de proteção apropriadas (secção A.8.1).

- **avaliação de risco** – a norma exige a avaliação e o tratamento do risco de segurança da informação de modo a permitir a preservação da confidencialidade, integridade e disponibilidade da informação (cláusulas 6. Planeamento e 8. Operação). Ora esta avaliação deve considerar um aumento do risco associado aos dados pessoais e as suas implicações financeiras, pois as multas previstas em caso de incumprimento do RGPD podem ter impactos financeiros significativos.

- **conformidade legal** – a NP ISO/IEC 27001:2013 exige o cumprimento com as obrigações legais, estatutárias, regulamentares e contratuais (secção A.18.1) e a realização de revisões à segurança da informação, de forma independente, em intervalos planeados ou sempre que ocorrerem alterações significativas (secção A.18.2).

- **classificação da informação** – o RGPD exige que os dados sejam tratados com a segurança apropriada, estando em sintonia com a norma que estabelece que a informação deve ser classificada e receber um nível adequado de proteção, de acordo com a sua importância para a empresa (secção A.8.2).

- **documentação** – o regulamento exige que sejam documentados elementos relevantes do processamento da informação, nomeadamente a identificação dos dados pessoais recolhidos, os fins para os quais as recolhas foram realizadas e o seu tratamento. A norma aborda o mesmo requisito, exigindo informação documentada na maioria das cláusulas do seu funcionamento, por exemplo sobre o âmbito do SGSI, a política de segurança, os processos de avaliação e de tratamento do risco, os objetivos de segurança, a competência dos recursos, a avaliação de desempenho do SGSI, os programas de auditoria e resultados. Uma cláusula é inteiramente dedicada à informação documentada (cláusula 7).

- **proteção desde a conceção** – o RGPD requer que mecanismos de segurança sejam aplicados desde o início do desenvolvimento (*privacy by design and by default*). A NP ISO/IEC 27001:2013 exige que a segurança da informação seja parte integrante dos sistemas de informação ao longo de todo o seu ciclo de vida (secção A.14.1)

- **relacionamento com fornecedores –** o RGPD aplica-se também a prestadores de serviços subcontratados, que efetuem o tratamento de dados pessoais em nome de terceiros, exigindo que os acordos formais contemplem a definição de medidas de segurança e limitações a esse tratamento. Por seu lado, a norma NP ISO/IEC 27001:2013 exige a proteção dos ativos da empresa que estão acessíveis aos fornecedores (secção A.15.1).

- **notificações às autoridades** – o regulamento exige que, em caso de incidentes com dados pessoais, as autoridades de supervisão sejam alertadas no prazo de 72 horas. A norma contempla um processo de gestão de incidentes para que eventos de segurança sejam documentados e relatados às autoridades o mais rápido possível, exigindo também que sejam mantidos os contatos adequados com as autoridades (secção A.16.1).

Requisitos do regulamento sobre o consentimento explícito, o direito ao "esquecimento" ou a nomeação do Encarregado de Proteção de Dados não são considerados na NP ISO/IEC 27001:2013, no entanto, como se pode verificar pelo acima exposto, esta norma é uma excelente referência que permite às empresas demonstrar o seu empenho e comprometimento com a segurança da informação.

A norma NIST analisada também se relaciona com o RGPD e com a norma NP ISO/IEC 27001:2013. Mais concretamente, a SP 800-61r2 recomenda para a gestão de incidentes que seja estabelecido e mantido um canal de comunicação adequado com a Administração da empresa e com as autoridades competentes, no sentido de notificá-las e mantê-las atualizadas sobre o desenvolvimento das ações em curso. Esta recomendação de reporte vai de encontro

ao estabelecido no RGPD para as notificações às autoridades, sempre que ocorram incidentes com dados pessoais.

A secção A.16 do Anexo A da norma NP ISO/IEC 27001:2013, que estabelece o objetivo de controlo para a gestão de incidentes de segurança da informação, recomenda que os controlos a aplicar incluam o estabelecimento de procedimentos e responsabilidades para assegurar uma resposta célere, eficaz e ordenada aos incidentes de segurança da informação, o reporte de eventos de segurança através dos canais de gestão apropriados, a deteção e reporte de pontos fracos nos sistemas ou serviços, a avaliação e decisão sobre se os eventos de segurança são incidentes, a resposta de acordo com procedimentos instituídos, a recolha de evidências e a aprendizagem com os incidentes ocorridos de forma a reduzir a probabilidade ou impacto de futuros incidentes. Constata-se que estas recomendações estão em harmonia com a NIST SP 800-61r2 e que as metodologias são muito semelhantes, não havendo diferenças significativas à parte da denominação dos processos.

Em suma, no que concerne à gestão da segurança da informação, a norma NP ISO/IEC 27001:2013 apresenta-se como a solução mais completa e abrangente, sendo a implementação de um SGSI um passo determinante para a conformidade com o RGPD. No entanto, os restantes modelos analisados oferecem também opções que podem ser aproveitadas e integradas no desenvolvimento e implementação de um SGSI, nomeadamente o modelo de capacidade de processos do COBIT 5 e os processos para a gestão de incidentes da SP 800-61r2.

Verifica-se que não há, efetivamente, um modelo melhor que outro, a questão reside em identificar qual o mais adequado para um contexto específico. Há, no entanto, desafios que se colocam à implementação da norma NP ISO/IEC 27001:2013, como sejam o compromisso da Administração da empresa, a adesão dos colaboradores aos novos processos e o seu contributo para o desenvolvimento de novas medidas.

Perante um cenário de decisão de implementação, a Administração deve expor claramente a todos os departamentos da empresa a importância e criticidade do SGSI e dos seus processos. Esta atuação é fundamental para que os colaboradores passem a ver a segurança da informação de forma relevante no desempenho das suas funções.

No mesmo sentido, a adesão dos colaboradores é indispensável para assegurar que os novos processos para a segurança da informação são encarados de forma séria e cumpridos de forma responsável. O envolvimento dos colaboradores no desenvolvimento de novas medidas permite reforçar a dimensão do sistema e promover a sua aplicação. Para facilitar esta adesão, devem ser promovidas sessões de divulgação e formação.

Como nota final ao estado da arte, importa salientar que a aquisição das normas internacionais ISO e da maioria dos materiais de certificação referenciados neste trabalho tem um custo significativo, que é, no entanto, compensado pela qualidade dos conteúdos apresentados.

3. CONTEXTO DO PROBLEMA

A 24 de agosto de 2004, através do Decreto Legislativo Regional n.º 27/2004/M, alterado pelos Decretos Legislativos Regionais n.^{os} 26/2013/M, de 29 de julho, 6/2015/M, de 13 de agosto e 42-A/2016/M, de 30 de dezembro, foi o Instituto de Habitação da Madeira transformado em entidade pública empresarial, atualmente denominada IHM – Investimentos Habitacionais da Madeira, EPERAM.

A IHM, EPERAM, doravante mencionada apenas pela sigla IHM, rege-se pelo seu diploma constitutivo, incluindo os seus estatutos, pelo seu regulamento interno e pelas normas legais que lhe são especialmente aplicáveis, nomeadamente as normas no domínio das empresas públicas regionais. É o organismo responsável pela implementação da política do Governo Regional da Madeira no domínio do apoio à habitação das famílias mais carenciadas e tem como objeto a promoção, o planeamento, a construção, a fiscalização e a gestão do parque habitacional e de outro património associado, assim como a realização de obras de recuperação, de construção e de reconstrução de habitações, de requalificação urbanística e de outras infraestruturas, especialmente no âmbito da habitação de interesse social. [58]

A operação da IHM na RAM é realizada na sede e na Loja do Cidadão, localizadas no Funchal, e em conjuntos habitacionais e polos comunitários situados em diversos concelhos[5]:

Funchal	Gabinete de Atendimento ao Público da Nazaré
	Conjunto Habitacional de Santo Amaro (Serviço de Fiscalização e Conservação)
	Conjunto Habitacional de Santo Amaro (Serviço de Habitação Social)
	Polo Comunitário Comandante Camacho de Freitas
Câmara de Lobos	Conjunto Habitacional da Palmeira
Santa Cruz	Conjunto Habitacional da Nogueira
Machico	Polo Comunitário da Torre
Porto Santo	Posto de Atendimento ao Cidadão

A IHM emprega atualmente 126 pessoas.

[5] São apresentados os locais onde há interligação de dados com a sede.

MISSÃO, VISÃO E VALORES

Missão Promover a melhoria contínua das condições habitacionais das famílias na Região Autónoma da Madeira, numa perspetiva global de integração social e de melhoria da qualidade de vida da população.

Visão Desenvolver a promoção da inclusão social com vista a minimização dos problemas habitacionais da Região.

Valores Dinamismo, transparência, proximidade e coesão. [59]

ORGANOGRAMA

A IHM é dirigida pelo Conselho de Administração (CA), constituído por uma Presidente e dois Vogais. A organização e funcionamento encontram-se assegurados por Regulamento Interno, aprovado pelo CA e publicado oficialmente.

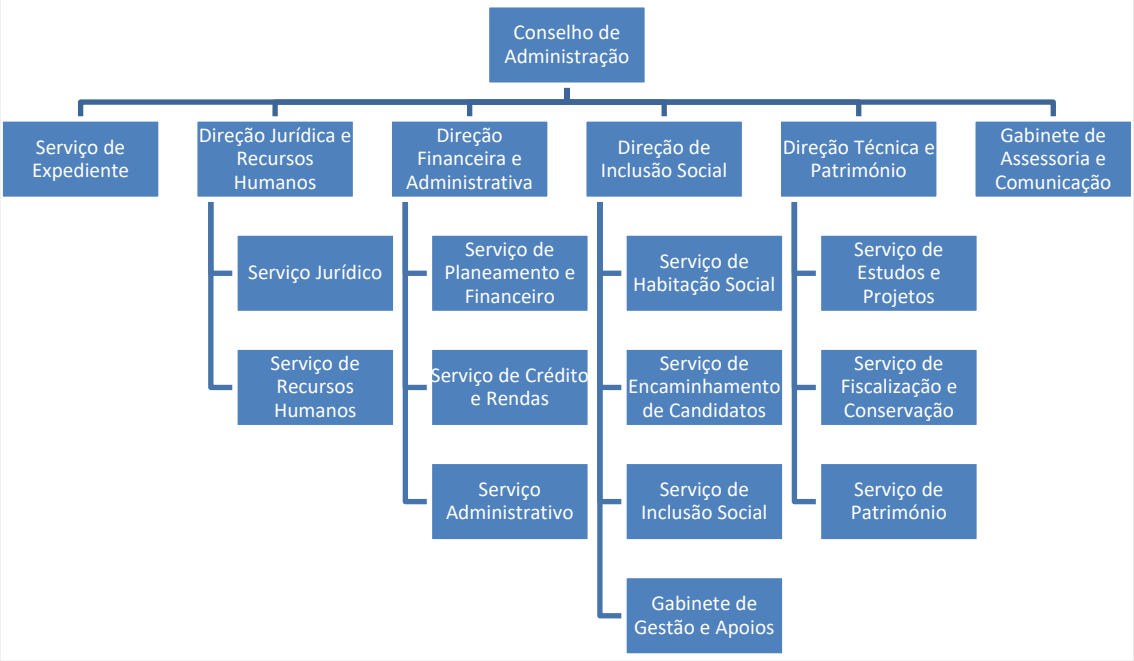


Figura 8 – Organograma da IHM [60]

PÚBLICOS

No domínio de atuação da IHM, os serviços prestados pela empresa coadunam-se com a diversidade das necessidades dos candidatos e dos beneficiários dos programas de apoio. Denominam-se beneficiárias as famílias contempladas com alguma forma de apoio e são considerados clientes aqueles a quem é faturado o serviço prestado pela IHM. Mantém, também, a IHM relacionamento institucional com diversas entidades públicas e privadas, regionais, nacionais e internacionais. Em todos estes casos, a veiculação de informação incluindo de dados pessoais é uma realidade, pelo que se consideram estas partes interessadas na segurança da informação recolhida e tratada pela IHM.

ÁREAS DE ATIVIDADE

Na prossecução das suas atribuições, a IHM desenvolve ações e presta serviços nas seguintes áreas principais:

- Reconstrução, aquisição e/ou construção de fogos para habitação social;
- Incremento dos apoios às famílias para recuperação das suas habitações;
- Reforço do programa de apoio na comparticipação de rendas e de prestações bancárias a desempregados;
- Dinamização de soluções de arrendamento habitacional;
- Desenvolvimento de ações de cooperação público-privada facilitadoras da satisfação das necessidades de habitação própria e de arrendamento;
- Implementação de projetos sociais com iniciativas próprias de inclusão social;
- Reforço das ações nos domínios da conservação e reabilitação do parque habitacional;
- Remoção das placas de fibrocimento com amianto das coberturas e varandas dos edifícios, substituindo-as por soluções energéticas eficientes;
- Limpeza, recuperação, dinamização e manutenção dos espaços verdes que integram os Conjuntos Habitacionais. [59]

3.1. SITUAÇÃO ATUAL

A estrutura organizacional da IHM e a atuação dos serviços em áreas tão distintas como a área financeira, jurídica, administrativa, social, entre outras, resultam na produção e circulação de uma grande variedade e elevado volume de informação, maioritariamente em formato digital.

Adicionalmente, da dispersão geográfica da empresa por vários concelhos da RAM para maior proximidade de atendimento e serviços sociais à população, emerge um panorama complexo em termos de sistema de comunicações e de segurança da informação transmitida entre os diversos locais e a sede.

Para melhor compreender esta realidade, procedeu-se a uma análise[6] empírica da situação atual, com particular atenção à existência de processos relacionados com a segurança da informação, definidos e implementados nos seguintes contextos:

Sobre a **organização** da empresa, observou-se os aspetos relacionados com a política de segurança, as responsabilidades sobre os ativos e a documentação operacional.

O estudo ao **ambiente físico** incidiu sobre as condições de segurança física das instalações da empresa, das áreas onde há operação de sistemas e a proteção das zonas específicas afetas ao processamento, tratamento e salvaguarda de informação.

[6] Por motivo de exigência de confidencialidade, a análise apresentada exclui detalhes técnicos e aspetos determinantes para a segurança da empresa.

A existência de **equipamentos** resultou na identificação e avaliação de máquinas e dispositivos existentes e nos aspetos relacionados com o manuseamento e com a segurança, enquanto ativos físicos tecnológicos.

A análise à **rede de dados** abrangeu a infraestrutura física, a cablagem, os sistemas de controlo de tráfego, a circulação e transferência de informação, a segurança das comunicações e a deteção e remoção de ficheiros maliciosos.

Para avaliação aos **sistemas aplicacionais** efetuou-se um levantamento sobre os programas informáticos utilizados, os ambientes de desenvolvimento, o acesso autorizado à informação, o armazenamento, os mecanismos de salvaguarda e o registo de *logs*.

No contexto do **pessoal,** analisou-se os ativos no que respeita às funções e responsabilidades, à segurança no término da relação contratual, à formação técnica e às atividades de sensibilização para a segurança.

A análise à **conformidade** aborda o cumprimento com requisitos legais e contratuais, nomeadamente os relacionados com a proteção de dados pessoais e a prestação de serviços que requerem acesso a informação digital.

3.1.1. Organização

A política de segurança é um instrumento que direciona a segurança de informação da empresa. Trata-se de um documento vital que reflete a disposição da Administração de dirigir a empresa de forma segura e controlada e que deve ser estabelecido e disponibilizado a todos os colaboradores, sendo revisto sempre que surjam novos requisitos ou algum objetivo de controlo não seja validado.

A IHM dispõe de alguns procedimentos de segurança estabelecidos, no entanto o conhecimento dos colaboradores sobre estes e sobre quem é responsável por cada procedimento não é global nem uniforme. Verificou-se também que, enquanto alguns instrumentos estão permanentemente disponíveis para consulta em plataformas *online*, tais como o "Regulamento Interno" ou o "Plano de Gestão de Riscos de Corrupção e de Infrações Conexas", outras apenas são comunicadas verbalmente ou por e-mail, por vezes sectorialmente, dando origem a que o conhecimento generalizado seja baseado no "passa palavra", que potencia interpretações incorretas e ambiguidades, podendo nem chegar ao conhecimento de todos os colaboradores.

De igual forma, o registo de ações de suporte técnico informático não se rege por um procedimento formal e rigorosamente executado, nem inclui a identificação de aspetos de segurança operacionalizados ou melhorados, fazendo assim prova insuficiente de cumprimento com qualquer objetivo de segurança, não contribuindo para a sensibilização dos colaboradores envolvidos sobre esta temática.

A título de exemplo, esta lacuna na definição de processos sobre a documentação operacional pode dar azo a falhas por incumprimento de etapas críticas, devido à inexistência de uma fonte que permita confirmar a forma de atuação correta.

Constatou-se, neste contexto, a carência de processos formalmente definidos e de uma política de segurança da informação abrangente, verificável e passível de melhoria contínua, que estabeleça claramente as regras a serem observadas nos diversos domínios da segurança da informação e que inclua os cargos e responsabilidades associados.

3.1.2. Ambiente Físico

A IHM ocupa instalações que cumprem parcialmente as exigências de segurança. A sede localiza-se num edifício de grande dimensão, onde operam outros serviços públicos e cuja manutenção técnica, nomeadamente ao nível da gestão da energia elétrica, é efetuada pela entidade gestora do prédio, cabendo à IHM apenas a manutenção da maioria dos espaços que ocupa.

Verifica-se nesse edifício a existência de um perímetro de segurança física, controlo de entrada física, sistema de videovigilância em todos os pisos e sistema de alarme. Estão igualmente instalados nas zonas comuns e operacionais do edifício equipamentos de controlo, deteção e segurança contra incêndio. No entanto, as portas interiores não dispõem de qualquer sistema de controlo de acesso e os vidros das janelas são facilmente quebráveis.

A zona crítica carateriza-se por um ambiente controlado e estanque, com porta corta-fogo que é mantida trancada para evitar qualquer acesso indevido. Apesar de apoiada por sistemas redundantes de energia elétrica e de ar condicionado, a área em questão requer normalização para cumprimento integral dos requisitos aplicáveis a *data centers*.

Outras áreas técnicas importantes, incluindo as de apoio à logística e ao suporte técnico, encontram-se em zonas não acessíveis ao público e comuns a outros serviços, carecendo de reconfiguração das delimitações dos espaços e de medidas de controlo de acesso para satisfazer as condições de segurança da infraestrutura e dos equipamentos.

As instalações da empresa fora da sede caracterizam-se por espaços controlados, existindo sistema de alarme e, em alguns casos, o reforço ao nível da resistência das janelas e portas. Não se enquadrando no âmbito das zonas críticas, estes locais dispõem, contudo, de ligações à rede de dados necessárias à operação dos serviços, cujos equipamentos devem ser servidos de redundância de energia elétrica. O controlo de acesso físico é normalmente realizado pelos colaboradores em serviço no local, o que está longe de ser o mecanismo adequado.

3.1.3. Equipamentos

O parque informático da IHM tem vindo a ser renovado em resultado de investimento na aquisição de equipamentos com caraterísticas adequadas às exigências de processamento e de

segurança da informação, com foco especial na desmaterialização de *hardware* e virtualização dos sistemas. Não obstante as vantagens desta solução, como a redução do consumo energético e a redução de risco por haver menor número de equipamentos a gerir, ainda se verifica um baixo nível de desempenho resultante de equipamentos em fim de vida útil ou não expansíveis, que requerem substituição com urgência.

Todos os ativos físicos tecnológicos são registados e catalogados aquando da sua aquisição, sendo identificáveis por código de barras e por consulta à base de dados. No entanto, verificou-se que em situações de término de relação contratual, embora em regra impere o bom senso na devolução de equipamentos e dispositivos móveis, não existe uma política que defina com exatidão os procedimentos para efetivar a sua recolha. Esta situação levanta problemas de segurança pois os equipamentos em causa podem conter informação relacionada com a empresa e com o trabalho realizado (e.g. mensagens de correio eletrónico institucionais e ficheiros descarregados), que passa a estar fora do controlo da empresa.

O manuseamento e as operações técnicas são efetuados por pessoal técnico habilitado com competências informáticas. É inexistente, contudo, uma política de operações que garanta a padronização dos mecanismos de segurança aplicados e que normalize o trabalho realizado. As intervenções técnicas estão, em geral, ao critério de cada técnico que, não obstante seguirem procedimentos aproximados, podem, inadvertidamente, incorrer em lapsos nas configurações, exatamente pela falta de documentação e de definição de políticas específicas para as operações.

Equipamentos eletrónicos obsoletos ou irreparáveis são tratados previamente ao processo de abate, sendo destruídos os dispositivos que possam conter informação. Ao prestador do serviço de abate é exigido o cumprimento das exigências ambientais aplicáveis. Equipamentos, componentes ou dispositivos reutilizáveis são armazenados para futura utilização, numa ótica de aproveitamento de recursos até ao limite da sua vida útil.

Os equipamentos são protegidos e, em geral, mantidos fora do alcance dos colaboradores, tanto quanto possível, exceto quando são por estes utilizados.

3.1.4. Rede de Dados

A IHM dispõe de uma infraestrutura de rede de dados com cablagem estruturada e serviços de comunicações que asseguram as ligações entre servidores e postos cliente na rede LAN, a interligação desta com locais remotos através de VPN segura e ligação redundante à internet. Estas ligações são de especial relevo, na medida em que a empresa dispõe de serviços descentralizados para maior proximidade com os cidadãos, o que exige a aplicação de mecanismos de segurança robustos na rede para o controlo de acesso, que permitam assegurar a autenticidade dos utilizadores que pretendem aceder aos sistemas, assim como a confidencialidade, integridade e disponibilidade da informação.

Com grande exigência em termos de disponibilidade, em virtude da implementação de sistemas amplamente acedidos por dezenas de utilizadores e de acessos à internet através de dipositivos móveis, o desempenho da rede revela a necessidade de maior velocidade para melhoria do desempenho atual.

De igual forma, não obstante a crucial importância dos sistemas de segurança implementados, o investimento na redundância, o desenvolvimento de um processo de certificação e a definição de uma política de rede são necessidades evidentes.

3.1.5. Sistemas Aplicacionais

A IHM proporciona o desenvolvimento interno de programas informáticos à medida das necessidades, a par da aquisição de soluções para diversas áreas funcionais. São realizadas avaliações prévias aos requisitos de desempenho, à exigência computacional e à segurança da informação. No entanto, verifica-se a inexistência de políticas para o levantamento de requisitos, para a aplicação de metodologias ágeis de desenvolvimento, para a gestão de alterações e para a documentação obrigatória de todas as aplicações.

Os mecanismos de segurança neste âmbito incluem a identificação e autenticação para acesso a programas e serviços, a gestão de privilégios e de palavras-passe. No entanto, o sistema centralizado de autenticação não é integralmente aproveitado por todas as aplicações, o que requer a utilização de múltiplas credenciais.

O armazenamento de dados em sistemas com redundância de discos, os mecanismos de substituição *hot-swap* que reduzem os tempos de recuperação em caso de avaria, assim como o funcionamento das aplicações numa arquitetura cliente-servidor são características de disponibilidade importantes utilizadas na empresa. No entanto, verifica-se a inexistência de uma classificação formal que valide a distinção das aplicações altamente críticas, críticas e não-críticas, por exemplo no que respeita aos requisitos de disponibilidade.

A classificação das aplicações decorre de interpretações percecionadas e não de um processo de avaliação com base em critérios que identifiquem, quantitativamente ou qualitativamente, o âmbito da aplicação, o número de utilizadores, o número de acessos diários ou o tipo e volume de dados tratados.

A configuração de *software*, incluindo de segurança, nos *end-points* segue normalmente uma *check-list* que estabelece quais os programas mais utilizados. No entanto, esta não se encontra normalizada, não existindo uma política de pré-configuração dos sistemas para cada área funcional da empresa, que permita uma reposição mais rápida dos sistemas em caso de avaria.

Verificou-se, também, que embora a maioria das aplicações efetue o registo de *logs* e os eventos de segurança, fundamentais para fins de auditoria, esta funcionalidade ainda não se encontra implementada em todos os sistemas.

3.1.6. Pessoal

O regulamento interno da IHM, conjugado com a legislação que define os conteúdos funcionais inerentes às diversas carreiras profissionais, estabelece as áreas de atuação dos serviços, assim como as funções e as responsabilidades dos colaboradores. No entanto, o referido regulamento não é extensivo ao âmbito da segurança da informação, denotando-se a ausência de uma política de responsabilidades neste domínio, que permita identificar quem têm autorização sobre o quê, ainda mais reforçada pela exigência de conformidade com o Regulamento Geral de Proteção de Dados.

A intenção dos ataques no ciberespaço e a sofisticação dos meios utilizados para ganhar algum tipo de vantagem não compadecem os atacantes perante empresas mal protegidas, cujo pessoal não é capaz de acompanhar os desafios de segurança por falta de formação. Escassas oportunidades para formação técnica, aliada à falta de planos específicos para técnicos e para programadores, potenciam o risco na medida em que estes poderão não conseguir atuar adequadamente perante um ataque.

De igual forma, não obstante a pedagogia realizada em contexto de apoio técnico aos colaboradores da empresa, verifica-se a falta de um plano de atividades de sensibilização para a segurança, que contemple os aspetos da confidencialidade, integridade, o não repúdio e outros princípios relacionados.

3.1.7. Conformidade

A IHM encontra-se abrangida pelo Plano de Ação para a Aplicação do Regulamento Geral de Proteção de Dados à Administração Pública Regional, da competência do Governo Regional da Madeira, que tem em curso uma série de processos com vista à conformidade com a esta legislação [9], que obriga a uma revisão do tratamento a dar aos dados pessoais de clientes, colaboradores, fornecedores e de outras entidades com quem a IHM tem acordos de parceria e associação.

O esforço para esta conformidade legal é grande, por força da dimensão da empresa, do volume de dados pessoais tratados e por não ter a IHM ainda estabelecido normas para a segurança da informação que ajudam a ultrapassar os desafios colocados pelo legislador.

As implicações deste regulamento na empesa incluem múltiplas alterações a procedimentos, regras e adaptações tecnológicas que venham a garantir a anonimização dos dados pessoais, o acesso mínimo indispensável aos colaboradores, a interoperabilidade entre sistemas e a permitir a notificação de incidentes. Os contratos existentes e futuros com prestadores de serviço têm de ser objeto de revisão, na medida em que estas entidades devem também estar em conformidade com a legislação.

Os serviços de suporte técnico a aplicações, realizados remotamente na maioria dos casos, exigem a atribuição de acesso aos sistemas e a definição de privilégios de leitura e escrita.

Estas intervenções, apesar de terem acompanhamento técnico por parte da equipa da IHM, requerem revisão e adequação dos controlos de segurança ao tipo de serviço prestado.

3.2. CONCLUSÕES

Em suma, a análise à situação atual indica que a IHM tem investido na melhoria de equipamentos, da infraestrutura e no desenvolvimento de aplicações que permitem uma melhor gestão de informação. No entanto, no âmbito da segurança da informação, a forma de atuação revela-se ainda predominantemente reativa, caracterizando-se pela falta de processos formalmente estabelecidos que imponham a aplicação de procedimentos especificados, orientados por requisitos de segurança e monitorizados para a deteção de falhas, que permitam a sua correção imediata. Um exemplo é algum do desenvolvimento aplicacional realizado, que não é regido por processos formais de aplicação de metodologias ágeis e de gestão de versões, cujo código não é auditado de forma independente, não sendo possível aferir os métodos aplicados.

Já sobre os processos informais existentes, constata-se que nem sempre são aplicados na íntegra e que a não uniformização de procedimentos dá lugar a que, por exemplo, dois ou mais colaboradores, ao realizarem tarefa idêntica, não executem os procedimentos na mesma ordem e com o mesmo rigor, assumindo muitas vezes os próprios a decisão do que é ou não é importante executar e implementar, dando azo a que, por omissão, sejam criadas vulnerabilidades adicionais.

Não tendo esta análise sido efetuada com base no Modelo de Capacidade de Processos do COBIT 5 resumido na Tabela 2, é, no entanto, percetível que a capacidade da maioria dos processos situa-se no nível 0. Esta conclusão deve reforçar a ambição da IHM de que processos inexistentes, mas necessários, devem ser formalmente criados e que os processos cuja execução não é completa sejam devidamente especificados, e que venham todos a atingir plenamente pelo menos o nível 1.

É notório que a não adoção de normas e modelos internacionalmente aceites, a existência de lacunas na sensibilização dos colaboradores e, em particular, a ausência de uma política de segurança de informação objetiva e mensurável, na prática está a impedir o eficaz planeamento, desenvolvimento e aplicação das melhores práticas existentes para este campo da tecnologia de informação, comprometendo o alavancar do desempenho do serviço informático da IHM, a proteção dos ativos e da informação, limitando a possibilidade de melhoria global dos serviços e da reputação da própria empresa.

4. ANÁLISE E METODOLOGIA

A análise à situação atual, apresentada no capítulo anterior, permitiu constatar que, embora a Investimentos Habitacionais da Madeira, EPERAM (IHM) tenha vindo a realizar investimentos importantes na área Informática, nomeadamente com a renovação de equipamentos, essa aposta não tem sido acompanhada do estabelecimento e implementação de processos de segurança de informação concretos, passíveis de avaliação e de melhoria, nem da definição de políticas de segurança que contribuam para minimizar ameaças, cuja finalidade é explorar vulnerabilidades e causar prejuízos significativos.

Para resolver este problema é necessária uma solução que permita garantir os aspetos de segurança fundamentais, nomeadamente assegurar que os ativos de informação da empresa apenas são acedidos por colaboradores autorizados e que efetivamente precisam da informação para o desempenho das suas funções, que a informação não é indevidamente alterada e que está sempre disponível quando necessária. Adicionalmente é necessário que a solução adotada permita atender às exigências de conformidade com os mais recentes instrumentos legais, nomeadamente o Regulamento Geral de Proteção de Dados (RGPD) [9] e a Diretiva para a Segurança das Redes e da Informação (NIS) [40].

A investigação ao estado da arte permitiu identificar uma norma internacional desenvolvida especificamente para a segurança da informação e já adaptada ao contexto nacional, que preconiza uma série de processos e ciclos iterativos de planeamento, implementação, verificação e melhoria, todos fundamentais para a proteção da informação: a NP ISO/IEC 27001:2013. Esta norma, que integra a metodologia que agora se propõe para a IHM, proporciona "os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação" (SGSI) [18, p. 6].

Sendo a NP ISO 27001:2013 composta por catorze secções e considerando que o tempo necessário para a sua completa implementação excede largamente o definido para este trabalho, optou-se por implementar quatro secções da norma, as que se entende serem as mais prementes face aos resultados da análise à situação atual e por terem impacto em projetos em curso, como é o caso da adaptação ao RGPD. Em concreto, as secções escolhidas foram:

- **Secção A.5 - Políticas de segurança de informação**, pelo facto das políticas serem documentos construídos a partir de necessidades identificadas, que permitem à empresa alcançar um padrão de proteção da informação adequado, através do estabelecimento de regras e normas de conduta, com o objetivo de diminuir a probabilidade da ocorrência de incidentes.
- **Secção A.12 - Segurança de operações**, pela necessidade de melhorar as operações sobre os recursos de informação, assegurando que os procedimentos são realizados de forma correta e segura. Esta secção atende a um leque alargado de tarefas técnicas realizadas na empresa, tais como a implementação de mecanismos de proteção contra código malicioso, realização de procedimentos de salvaguarda de dados,

monitorização, controlo de instalação de *software*, gestão de vulnerabilidades, atividades de auditoria, entre outros.

- **Secção A.13 - Segurança de comunicações**, atendendo às necessidades de proteção da informação em circulação na rede local (LAN) e nas redes privadas virtuais (VPN) da empresa. Esta secção aborda também a necessidade de políticas para a transferência de informação, os acordos com entidades externas e as mensagens eletrónicas, que carecem de revisão, nomeadamente para cumprimento do RGPD.
- **Secção A.16 - Gestão de incidentes de segurança da informação**, para o estabelecimento de controlos de deteção, avaliação e reporte de incidentes, assim como de recolha de evidências. Os procedimentos associados a esta gestão permitem cumprir com o requisito de notificação de incidentes imposto pelo RGPD, assim como obter conhecimentos para melhorar os controlos aplicados no sentido de minimizar ocorrências futuras.

A implementação das secções mencionadas não pode, contudo, ser iniciada sem que antes se proceda à execução de um conjunto de processos de planeamento que permitem conhecer e avaliar com detalhe os recursos de informação da IHM, nomeadamente ao nível do risco, de forma a fundamentar e a especificar, correta e adequadamente, os controlos necessários para a fase de implementação.

4.1. PROCESSOS

Ao proporcionar "os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação" (SGSI) [18, p. 6], a norma NP ISO 27001:2013 sugere uma sequência de processos de planeamento, implementação, avaliação e melhoria, cujo diagrama se adaptou do ISO27K Forum Version 4 (2016) [61] e se apresenta na ***Figura 9***, com melhor visibilidade no Anexo III.

A primeira adaptação efetuada consistiu em aplicar o ciclo PDCA – *Plan* – *Do* – *Check* – *Act,* através de um esquema cromático, que faz corresponder uma cor específica ao tipo de processo:

Processos de planeamento (*Plan)*

Processos de implementação (*Do*)

Processos de avaliação (*Check*)

Processos de melhoria (*Act*)

A segunda adaptação foi a inclusão no diagrama de duas componentes fundamentais para a segurança da informação: os processos para Gestão do Risco e os processos para Gestão de Incidentes, isto porque na fonte mencionada [61] apenas constava dos artefactos operacionais

uma breve indicação da existência de métricas e de incidentes, não existindo, contudo, qualquer detalhe sobre como chegar à obtenção das métricas nem como proceder em relação aos incidentes, o que se considerou ser manifestamente insuficiente para este trabalho, atendendo a que a segurança da informação assenta nos processos de gestão ora introduzidos, justificando, assim, a adaptação realizada.

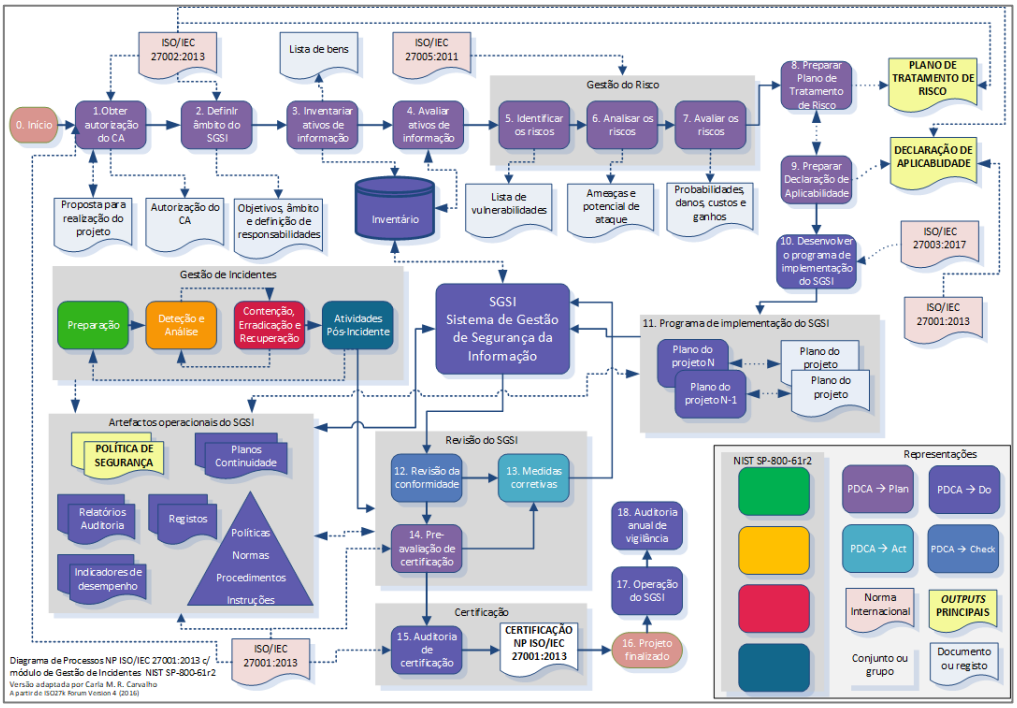


Figura 9 – Diagrama de Processos, adaptado de ISO27K Forum Version 4 (2016) [61]*, e com melhor visibilidade no Anexo III.*

A interligação dos processos é estabelecida num esquema lógico em consonância com o ciclo PDCA – *Plan, Do, Check, Act*, anteriormente representado na ***Figura 1***. Através do esquema de cores referido é dado o enquadramento de cada processo nas fases do ciclo, sendo que as ligações entre os processos, numerados sequencialmente, indicam a ordem de execução. São também indicados os documentos produzidos em cada processo, as normas auxiliares envolvidas e destacados os principais *outputs*: o Plano de Tratamento do Risco, a Declaração de Aplicabilidade e as Políticas de Segurança da Informação.

O diagrama representa o guião completo de implementação da norma NP ISO/IEC 27001:2013 a seguir neste trabalho, que se inicia com a fase de planeamento, cujos processos iniciais se destacam na ***Figura 10***. O primeiro processo consiste na obtenção de autorização do Conselho de Administração (CA) da IHM para a realização do projeto. Obtida a autorização, é necessário definir o âmbito do SGSI, ou seja, qual a abrangência do sistema, quais os objetivos que este deve atingir e quais as responsabilidades dos intervenientes (processo 2).

Sendo os ativos de informação da IHM objetos centrais no SGSI, o processo seguinte consiste, naturalmente, na inventariação desses ativos (processo 3), onde se pretende identificar o tipo de ativos existentes e especificar a metodologia utilizada na recolha da informação.

Identificados os ativos de informação, segue-se a sua avaliação (processo 4), atendendo a critérios como o valor de aquisição ou de contratação, o valor da informação ou em termos do tempo de reparação e de paragem das atividades, entre outros. Apesar de este processo não fazer parte da norma, decidiu-se pela sua integração no diagrama por se considerar importante para a análise de impacto no processo seguinte. Entende-se que, se o valor de um ativo é muito baixo, então a ocorrência de um incidente sobre esse ativo teria, normalmente, pouco impacto na empresa. Já um incidente envolvendo a vida humana, por exemplo, acarretaria um impacto inestimável.

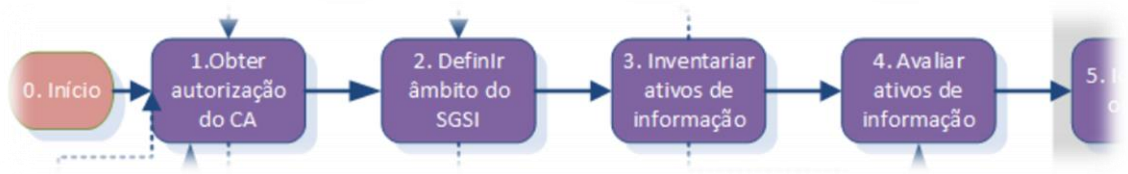


Figura 10 – Extrato dos processos iniciais de planeamento no Diagrama de Processos

A identificação e avaliação realizadas nos dois processos anteriores são essenciais para a execução do processo seguinte, um dos principais no esquema apresentado: o processo de Gestão do Risco. Este processo engloba três subprocessos: a identificação dos riscos associados aos ativos decorrente de vulnerabilidades identificadas (processo 5), a análise desses riscos em termos de ameaças e potencial de ataque (processo 6) e a avaliação dos riscos atendendo às probabilidades de ocorrência e ao impacto estimados (processo 7).

Na sequência dos processos referentes à Gestão do Risco surge a preparação do Plano de Tratamento do Risco (processo 8), que é um dos três mais importantes documentos para a implementação da norma NP ISO/IEC 27001:2013. Este documento estabelece para cada ameaça qual o(s) controlo(s) a aplicar, a prioridade de intervenção, quem implementa, quando o faz, qual o prazo e qual o custo de implementação.

Apesar da elevada importância do Plano de Tratamento do Risco, este não é suficiente para a conformidade com a norma NP ISO/IEC 27001:2013, que requer a preparação de outro documento fundamental (processo 9): a Declaração de Aplicabilidade, que é composta obrigatoriamente por todos os controlos genéricos que compõem o Anexo A da norma, podendo ser complementada com outros controlos específicos. Esta Declaração deve indicar quais os controlos aplicáveis à empresa, informar se já estão implementados ou não, esclarecer sobre a implementação realizada e justificar os motivos para a sua inclusão ou exclusão.

Com o processo anterior termina a fase de planeamento - fase "*Plan*" - do ciclo PDCA. Esta fase é, no entanto, retomada mais adiante num processo específico relacionado com a revisão do SGSI para efeitos de certificação.

No seguimento, surge o primeiro processo da fase de implementação - fase "Do" - que é o desenvolvimento do programa de implementação do SGSI (processo 10). Este processo recorre aos processos da fase de planeamento para estabelecer uma *checklist* das atividades de

implementação, que ajuda a monitorizar o progresso ao longo do tempo. Neste processo é também definida a estrutura da Política de Segurança, que é o terceiro documento fundamental da norma NP ISO/IEC 27001:2013.

O programa de implementação do SGSI (processo 11) estabelece os planos para os projetos a implementar, ou seja, define a implementação das secções da norma escolhidas anteriormente e os respetivos controlos. Para cada controlo são definidos atributos de informação, entre os quais a medição a efetuar, a fórmula ou pontuação a utilizar e o alvo pretendido. Estes dados são importantes para a monitorização a realizar posteriormente.

Concluído o programa de implementação, inicia-se a fase de avaliação - fase "Check" – com a revisão da conformidade do SGSI (processo 12), que atende ao indicador de desempenho de cada controlo e à confrontação com a política de segurança. Este processo impõe uma análise crítica e a revisão da política de segurança, caso se detete a necessidade de endurecimento das regras aplicadas.

A aplicação de ações corretivas e de prevenção (processo 13) aos controlos cujos indicadores não apresentam resultados satisfatórios, visam a melhoria contínua do SGSI e caracterizam a fase "Act" do ciclo PDCA. Este processo é fundamental para que o sistema se mantenha atualizado e capaz de dar resposta às ameaças que sobre ele recaem.

À parte dos processos mencionados anteriormente, o diagrama apresenta outras áreas importantes:

- a Gestão de Incidentes, destacada na ***Figura 11***, que contém processos para preparar, detetar e analisar, conter erradicar e recuperar de incidentes, e realizar atividades pós-incidente de segurança, recomendados pela norma SP-800-61r2 do *National Institute for Standards and Technology* (NIST). A integração com a norma ISO/IEC 27001:2013 é possível pois são processos que vão de encontro aos seus requisitos e permitem a ligação com a revisão do SGSI. Tal como referido no estado da arte a este respeito, as metodologias existentes para a gestão de incidentes são semelhantes, variando quase sempre e apenas a denominação dos processos. A ligação entre a gestão de incidentes e o SGSI decorre da ocorrência de um incidente implicar uma revisão do sistema para aplicação de medidas corretivas adequadas.

Figura 11 – Extrato dos processos para a gestão de incidentes no Diagrama de Processos

- os Artefactos Operacionais do SGSI, como se pode observar na ***Figura 12***, incluem grande parte dos documentos e registos produzidos e fazem parte dos requisitos da norma, nomeadamente para fins de prova em caso de auditoria.

Figura 12 – Extrato dos artefactos operacionais do SGSI no Diagrama de Processos

A certificação da IHM em NP ISO 27001:2013 requer um processo de pré-avaliação de certificação (processo 14), decorrente da revisão de conformidade. Trata-se de um processo de planeamento para a realização da auditoria de certificação (processo 15). Obtida a certificação, o projeto é dado como finalizado (processo 16). A normal operação do SGSI (processo 17) requer, no entanto, um processo de auditoria anual de vigilância (processo 18).

Apresentado o guião da arquitetura proposta, são, em seguida, detalhados os processos da fase inicial de planeamento:

4.1.1. Obter Autorização

A norma NP ISO 27001:2013 esclarece que "a adoção de um sistema de gestão de segurança da informação é uma decisão estratégica da organização" [18, p. 5]. Neste sentido, previamente ao início deste trabalho, mesmo não estando ainda definida qual a metodologia que seria seguida foi solicitada autorização ao Conselho de Administração da IHM (CA) para a realização deste projeto, a qual mereceu parecer favorável.

4.1.2. Definir Âmbito do SGSI

Obtida a autorização do CA, foi estabelecido o âmbito e definidos os objetivos do SGSI, que incluem as quatro secções da norma NP ISO 27001:2013 propostas no início do presente capítulo: A.5 – Políticas de segurança de informação, A.12 - Segurança de operações, A.13 - Segurança de comunicações e A.16 - Gestão de incidentes de segurança da informação.

Também é parte integrante deste processo a definição das funções e responsabilidades de segurança na organização. A cláusula 5.3 da norma ISO/IEC 27001:2013 explicita que "a gestão de topo deve assegurar que são atribuídas e comunicadas as responsabilidades e autoridades para funções que são relevantes para a segurança da informação" [18, p. 8].

Adicionalmente, o ponto 5.3.2 da mesma cláusula e o Anexo B da norma ISO/IEC 27003:2010, que guia a implementação de um SGSI, indicam as mais importantes considerações a ter na definição de funções na gestão da segurança da informação:

- A responsabilidade geral pelas tarefas permanece ao nível da gestão;
- É nomeado um responsável para promover e coordenar o processo de segurança da informação;
- Cada colaborador é igualmente responsável pelas suas tarefas e pela manutenção da segurança da informação no local de trabalho e na organização. [20, p. 16]

Também o RGPD estabelece na secção 4 - artigo 37º a figura do Encarregado da Proteção de Dados [9], responsável por informar e aconselhar a Administração da empresa sobre todos os aspetos relacionados com a proteção de dados, controlar a implementação de medidas e realizar os procedimentos internos necessários à conformidade e de comunicação com a autoridade (Comissão Nacional de Proteção de Dados).

No Anexo V apresenta-se uma descrição das funções e responsabilidades relacionadas com a segurança da informação, indicando as funções existentes na IHM.

4.1.3. Inventariar Ativos de Informação

A inventariação dos ativos de informação da IHM passou, em primeiro lugar, pela compreensão da definição de "ativo" no contexto da informação.

Segundo Oppenheim, Stenson e Wilson [62]:

"Ativos de informação são recursos que são ou devem ser documentados e que garantem benefícios económicos futuros."

Atendendo a que estes ativos são os elementos para os quais será feita a identificação de vulnerabilidades e potenciais ameaças e calculado o risco associado, a norma NP ISO 27001:2013 esclarece que "devem ser identificados os ativos associados com a informação e os recursos de processamento de informação e deve ser mantido um inventário destes ativos" (secção A.8.1.1), que "os ativos registados devem ter um responsável" (secção A.8.1.2) e que deve ser estabelecida a "utilização aceitável de ativos" (secção A.8.1.3) [18, p. 18].

Paralelamente, a norma auxiliar ISO/IEC 27005:2011 estabelece no seu Anexo B [22, p. 33] que dois tipos de ativos podem ser distinguidos: **ativos primários**, que incluem os processos de negócio e atividades, e a informação; e **ativos de suporte e infraestrutura**, entre os quais se encontram o *hardware*, o *software*, a rede, os recursos humanos, as instalações físicas e a própria organização. O processo de inventariação de ativos da IHM incidiu na recolha de dados sobre estes dois tipos de ativos, considerando aqueles que são úteis para a elaboração da política de segurança da informação.

A título de exemplo, para os ativos primários considerou-se o processo de realização de cópias de segurança da informação na medida em que o seu não cumprimento e posterior verificação pode afetar significativamente o funcionamento da IHM, caso se verifique a necessidade de reposição de dados. Já sobre a informação, foi inventariada a informação digital fundamental

para o funcionamento da empresa e a informação cujo custo é elevado devido aos longos períodos de recolha, armazenamento ou processamento. O levantamento de dados pessoais, no âmbito da legislação da proteção de dados, está a decorrer no momento da realização deste trabalho.

O inventário dos ativos de suporte e infraestrutura, incluiu os seguintes elementos:

- ***Hardware***, tais como computadores pessoais, portáteis, servidores, impressoras, discos de rede, unidades de disco amovíveis e cartões de memória.
- ***Software***, como sejam sistemas operativos, aplicações específicas (desenvolvidas à medida), soluções padrão (e.g. *Enterprise Resource Planning* (ERP)), soluções *Software as a Service* (SaaS), *software* de virtualização e utilitários *freeware*.
- **Infraestrutura**, considerando o suporte a cablagem, os equipamentos e as interfaces de comunicação e os protocolos que permitem a interconexão dos sistemas de informação, como sejam os *switches*, *routers* e os serviços instalados (e.g. filtragem, auditoria), assim como a possibilidade de administração remota (e.g. iLO, RD, VNC, Teamviewer).
- **Recursos humanos**, considerando os decisores e dirigentes (responsáveis pelos ativos primários), os utilizadores que possuem acesso aos sistemas para tratamento da informação, e a equipa informática, que possui acesso privilegiado aos sistemas para desempenho das suas funções.
- **Instalações físicas**, considerando o ambiente externo, o edifício e as zonas internas, os serviços essenciais (e.g. energia elétrica), serviços de infraestrutura (e.g. climatização), os serviços de comunicação e o meio físico.
- **Organização**, que contempla as entidades com autoridade sobre a IHM (e.g. Governo Regional), a estrutura organizacional da empresa, a organização de projetos e as entidades contratadas para fornecimento de serviços ou recursos (e.g. serviços disponibilizados na nuvem, serviços de suporte técnico e serviços de assessoria).

Para a recolha desta informação foram aplicadas as técnicas de observação participante, análise documental e entrevista semiestruturada. Optou-se por estes métodos por estarem reunidas as melhores condições possíveis para a obtenção de informação, atendendo ao desempenho de funções profissionais da autora nesta empresa.

OBSERVAÇÃO PARTICIPANTE

Este método de observação imersa no ambiente da IHM decorreu dia-a-dia nas atividades de suporte técnico e de interação com os sistemas e utilizadores e revelou-se o método mais enriquecedor, na medida em que resultou na mais próxima recolha e análise de dados que é humanamente possível realizar.

ANÁLISE DOCUMENTAL

A análise a documentos relacionados com a temática deste trabalho recaiu sobre os seguintes instrumentos:

- Estatutos da IHM;
- Regulamento Interno;
- Plano de Gestão de Riscos de Corrupção e de Infrações Conexas;
- *Check-list* de procedimentos para instalação de postos de trabalho;
- Processo de realização de cópias de segurança dos dados;
- Plano de arquitetura da rede local e *VPNs;*
- Lista de recursos humanos;
- Manual de boas práticas no âmbito da informática: utilização da rede, do correio eletrónico, da Internet, de impressoras, pastas partilhadas e armazenamento de dados.

ENTREVISTA SEMIESTRUTURADA

Foram realizadas entrevistas a colaboradores e dirigentes da IHM no sentido de se obter o melhor conhecimento sobre os processos organizacionais, recursos envolvidos, ameaças identificadas e situações passíveis de melhoria.

No processo de inventariação efetuado considerou-se como responsável por um ativo a pessoa que realiza operações com esse ativo e atende à segurança de informação no mesmo. Quando um ativo é utilizado por vários colaboradores, a responsabilidade recai sobre o dirigente associado à natureza do ativo. No caso dos recursos humanos, tomou-se como responsável o chefe de serviço na medida em que é quem gere a equipa na sua dependência.

Concluído este processo, constatou-se que a IHM, no contexto da RAM, possui um parque informático de pequena/média dimensão a nível de *hardware*, *software* e infraestrutura de rede, suportado por uma equipa técnica experiente, mas composta por poucos elementos. O seu valor é, no entanto, bastante elevado em virtude da natureza e volume da informação tratada nas diversas áreas de atuação da empresa.

4.1.4. Avaliar Ativos de Informação

Identificados os ativos de informação da IHM e os seus responsáveis, realizou-se uma avaliação destes recursos com o objetivo de se obter indicadores do nível de risco associado a cada ativo. Foram considerados os critérios:

- **Valor da vida humana**, em observação às condições de segurança para os recursos humanos que operam os ativos;
- **Valor de aquisição ou de contratação**, no contexto do investimento efetuado;
- **Valor da informação**, atendendo à sua criticidade para o funcionamento da empresa e à propriedade intelectual;
- **Tempo de reparação**, associado a necessidades de manutenção dos equipamentos;
- **Tempo de paragem das atividades**, tendo em conta os custos operacionais em virtude da inoperacionalidade dos ativos;
- **Imagem interna**, reflexo da satisfação dos colaboradores da empresa;
- **Reputação da empresa no exterior**, atendendo à imagem institucional junto de clientes, fornecedores, parceiros, e outras entidades;

A avaliação dos ativos de informação foi importante no sentido de se poder dispor de dados quantitativos que permitam perceber quais são os bens de maior valor, aos quais estará associado um impacto maior em caso de incidente.

Para se estimar o impacto de um incidente é fulcral desencadear o processo de gestão do risco, que utiliza precisamente os ativos inventariados para identificar vulnerabilidades e ameaças e calcular o risco de modo a que um tratamento adequado possa ser, posteriormente, estabelecido.

4.1.5. Gestão do Risco

Empresas detentoras de informação alvo de interesse estão sujeitas a ataques que podem ter efeitos negativos e altamente lesivos em termos de desempenho económico, reputação, segurança, aspetos sociais, entre outros. Sem gestão e tratamento adequados, o risco de perda de informação pode tornar-se um risco de transferência de conhecimento para o atacante.

A norma NP ISO/IEC 27001:2013 estabelece que o sistema de gestão de segurança da informação (SGSI) “preserva a confidencialidade, integridade e disponibilidade da informação através da aplicação de um processo de gestão do risco” [18, p. 5]. Assim, o planeamento do SGSI para a IHM contemplou a gestão e tratamento do risco em alinhamento com os princípios

e diretrizes das normas ISO/IEC 27005:2011 [22] e ISO/IEC 31000:2012 [23], ambas dedicadas a este campo de ação.

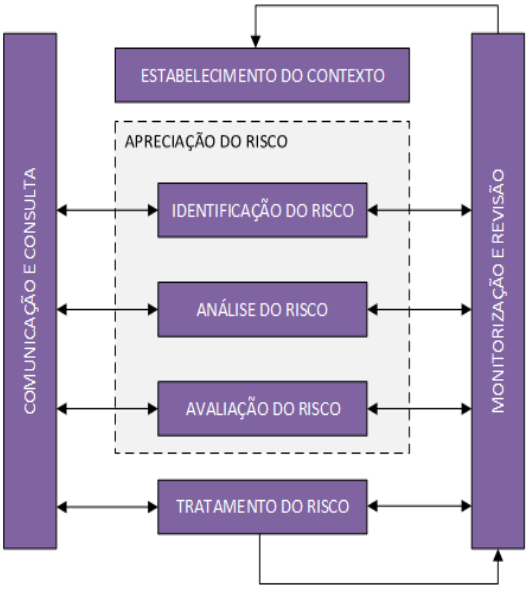


Figura 13 – Processo de Gestão do Risco **[23, p. 21]**

A Gestão do Risco é a etapa mais importante da fase de planeamento, pois é aqui que são estabelecidos os alicerces para a segurança da informação. Este processo, representado na ***Figura 13*** [23, p. 21], tem como propósito a redução da probabilidade de ocorrência de eventos danosos à segurança da informação, assim como a minimização do seu impacto, através de um ou mais ciclos iterativos que permitem identificar, analisar, avaliar e tratar os riscos.

O processo tem início com a definição do contexto, que neste trabalho é o suporte ao SGSI, onde se inclui o estabelecimento do(s) critério(s) de aceitação do risco residual. Para a IHM, propõe-se que o risco seja aceitável quando o custo do dano for inferior ao custo de mitigação do risco. Seguiu-se o processo de apreciação do risco, composto por três etapas: identificação, análise e avaliação.

IDENTIFICAR OS RISCOS

A identificação do risco consistiu em determinar quais os acontecimentos que podem causar perda de confidencialidade, integridade e disponibilidade da informação**.** Com base na inventariação dos ativos apuraram-se as vulnerabilidades e ameaças, a fonte e as respetivas consequências (Anexo VI).

A cláusula 8.3.2 da norma ISO/IEC 27005:2011 indica que "convém que as consequências expressas em tempo e valor financeiro sejam medidas com a mesma abordagem utilizada para a probabilidade da ameaça e para as vulnerabilidades. A consistência deve ser mantida com respeito à abordagem quantitativa ou qualitativa" [22, p. 29]. Por este motivo, a expressão das

consequências no referido anexo segue a nomenclatura “Probabilidade / Impacto”, tendo-se aplicado valores estimados, apresentados na Tabela 3 e

Tabela 4.

ANALISAR OS RISCOS

Para a análise do risco optou-se pela metodologia quantitativa. Este método é vantajoso face à análise qualitativa, cuja escala é subjetiva. A indicação de valores monetários facilita a tomada de decisão. Assim, foram definidas escalas com valores numéricos:

- quanto à probabilidade de ocorrência, em que quanto mais elevada a probabilidade de ocorrência, maior a classificação;
- quanto ao impacto, em termos de custo/dano/ganho verificado, em que quanto mais elevado seja o impacto, maior a classificação;

Tabela 3 - Escala de probabilidades

Classificação	Probabilidade de ocorrência
1	1 vez em 10 000 anos
2	1 vez em 1000 anos
3	1 vez em 100 anos
4	1 vez em 10 anos
5	1 vez por ano
6	1 vez por mês
7	1 vez por semana
8	1 vez por dia
9	1 vez por hora
10	1 vez por minuto

Tabela 4 - Escala de impacto

Classificação	Impacto (custo/dano/ganho)
1	0,10 €
2	1 €
3	10 €
4	100 €
5	1.000 €
6	10.000 €
7	100.000 €
8	1.000.000 €
9	10.000.000 €

10	danos totais

A análise do risco realizada combina a estimativa da probabilidade de ocorrência com o impacto resultante. São exemplo de ameaça as duas situações apresentadas na Tabela 5:

Tabela 5 - Análise do risco (exemplos)

Tipo	Ameaça	Fonte	Probabilidade / Impacto
Ação não autorizada	Instalação não autorizada de *software*	Intencional	5/7
Falha técnica	Falha de equipamento de comunicação	Acidental	4/7

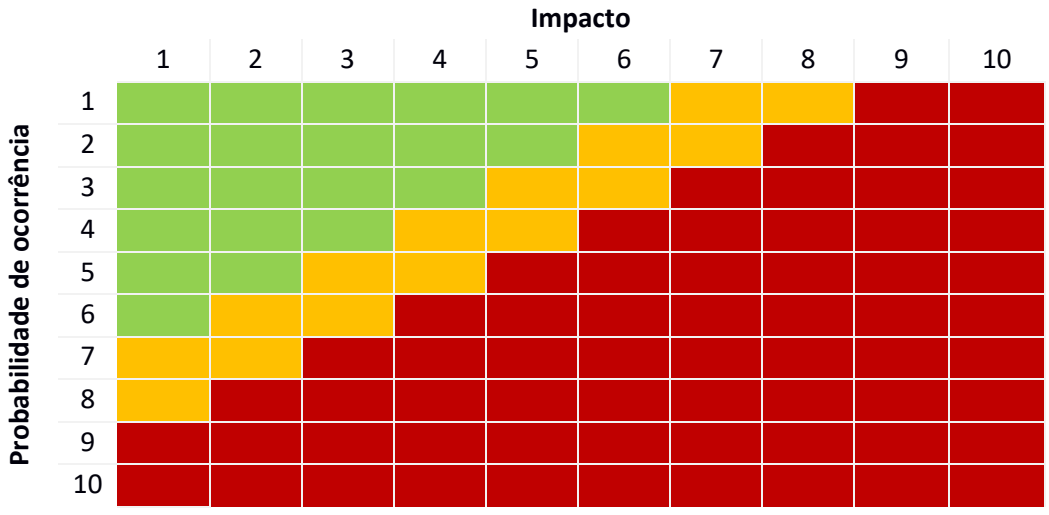
A probabilidade de ocorrência de uma ação não autorizada, como é o caso da instalação não autorizada de *software*, apesar de pouco provável, pois requer privilégios de administração na máquina, deve ser considerada na medida em que representa um risco de infeção do equipamento se for de fonte desconhecida e uma falha no processo de licenciamento de *software* com custos na ordem da centena de milhar de euros (dependendo do número de instalações).

Já a falha de um equipamento de comunicação poderia ter um custo na mesma ordem de valor, no entanto estima-se ser uma ameaça menos frequente pois o histórico de falhas neste tipo de equipamentos assim o indica e a sua natureza é, normalmente, acidental.

AVALIAR OS RISCOS

Para avaliar os resultados da análise do risco foi definida uma **Matriz de Risco:**

Tabela 6 - Matriz de Risco



O esquema cromático da Tabela 6 ilustra a intersecção das classificações de ambas as escalas (**Probabilidade x Impacto**) e facilita a identificação dos níveis de risco: riscos residuais (verde, entre 1 e 6), riscos médios (laranja, entre 7 e 8) e riscos elevados (vermelho, entre 9 e 10). Para cada nível de risco foi definida a prioridade de intervenção e estabelecido um prazo adequado à sua realização.

As prioridades de intervenção e os prazos propostos na Tabela 7 requerem, contudo, explícita e impreterivelmente, aprovação da Administração da empresa. Esta condição decorre de, por exemplo, numa situação de restrição orçamental que implique o adiamento da implementação de medidas de segurança, poder-se cumprir com o estabelecido na norma NP ISO/IEC 27001:2013 sobre a responsabilidade pela segurança da informação da empresa que é da Administração.

Tabela 7 - Nível do risco, intervenção e prazo de atuação

Nível do Risco	Intervenção	Prazo
Residual	Não prioritária (médio-prazo)	3-6 meses
Médio	Agendada (curto-prazo)	1-2 meses
Elevado	Prioritária	Imediato

A importância de cada risco é essencial para o processo de tratamento, devendo ser prioritários não apenas os riscos mais prementes, mas também os tratamentos mais facilmente executáveis, sendo o prazo de intervenção definido consonante com a prioridade.

Cada avaliação realizada deve produzir resultados sólidos, válidos e comparáveis, pois cumprindo-se o ciclo PDCA será necessário reavaliar os riscos periodicamente, em particular quando ocorrem ou são propostas alterações significativas. Para cada risco que não seja aceitável, um ou mais controlos do Anexo A da norma NP ISO/IEC 27001:2013, ou outros que a empresa estabeleça, devem ser aplicados, calculando-se de novo o risco após a sua implementação.

Num ambiente complexo e repleto de ameaças e incertezas como é o ciberespaço, a gestão do risco ajuda a estabelecer um bom nível de segurança na empresa, na medida em que reúne as condições para a preparação de um **Plano de Tratamento de Risco**.

4.1.6. Plano de Tratamento do Risco

A norma ISO/IEC 27005:2011 estabelece quatro opções para o tratamento do risco:

1. **Modificação do risco**, através da implementação de controlos de segurança que permitem a sua correção, eliminação, prevenção, minimização do impacto, dissuasão, deteção, recuperação, monitorização e consciencialização;

2. **Partilha do risco**, através da sua transferência para terceiros, por exemplo através de uma apólice de seguro;
3. **Evitação do risco**, por alteração completa do modo de realizar uma atividade, ou mesmo cancelando-a para evitar o risco;
4. **Aceitação / Retenção do risco**, quando o nível de risco reflete o critério de aceitação; [22, p. 35]

A decisão por uma ou mais opções para o tratamento de um risco é perfeitamente possível pois verifica-se que, por exemplo, tentar evitar um risco alterando a forma de atuação não invalida que esse mesmo risco possa estar seguro através de uma apólice. O tratamento do risco consiste em avaliar se o nível de risco do tratamento escolhido é aceitável ou não. Se não for, um novo tratamento terá de ser definido, caso contrário é feita uma avaliação ao tratamento realizado.

Para operacionalizar o tratamento do risco foi elaborado um dos principais *outputs* do SGSI: o **Plano de Tratamento do Risco**, detalhado no Anexo VII. Este plano define para cada ameaça qual o controlo aplicável, a prioridade de intervenção, quem o implementa, quando o faz, qual o prazo de implementação e o custo. Sendo a implementação deste plano exigente em termos de tempo, de investimento e de esforço, caso o número de controlos seja elevado, o plano deve ser previamente submetido a aprovação por parte da Administração antes da sua aplicação prática.

Para as duas situações exemplificadas na Tabela 5, apresenta-se na Tabela 8 um resumo do tratamento a realizar, indicando controlos passíveis de aplicação:

Tabela 8 - Tratamento do risco (exemplos)

Ameaça	Controlo a implementar	Descrição do controlo	Detalhe da implementação	Prioridade de intervenção
Instalação não autorizada de *software*	A.12.5.1	Instalação de *software* nos sistemas de produção	Os utilizadores com privilégios para instalação de *software* devem registar em formulário todas as instalações efetuadas, o respetivo nº de licença, os postos e utilizadores do *software* e fundamentar a instalação.	Prioritária
Falha de equipamento de comunicação	A.13.1.1	Controlos de rede	Verificar a ligação do equipamento à rede, rever as configurações, os serviços e os protocolos utilizados.	Prioritária

Dada a criticidade da proteção da informação para a IHM, informações sobre os riscos e o tratamento a aplicar devem fazer parte da comunicação interna ao pessoal técnico e aos

dirigentes com responsabilidades nesta área de atuação, com o intuito de alertar, ajudar a prevenir e até, eventualmente, lidar com eventuais ocorrências não antecipadas.

Duas atividades finalizam o processo de gestão do risco: a comunicação e consulta, que contempla os "processos contínuos e iterativos que uma organização conduz de forma a fornecer, partilhar ou obter informações, e para se envolver em diálogo com as partes interessadas no que respeita à gestão do risco" [23, p. 11]; e a monitorização e revisão, para que se identifiquem, tão breve quanto possível, eventuais alterações no contexto da organização e seja possível manter uma visão global dos riscos.

O mapeamento entre as etapas do processo de gestão do risco e as quatro fases do ciclo PDCA que caracterizam o estabelecimento, a implementação, a manutenção e a melhora contínua de um sistema de gestão de segurança da informação, é sintetizado na Tabela 9 [23, p. 16]:

Tabela 9 - Mapeamento entre o Processo de Gestão do Risco e o ciclo PDCA

Ciclo PDCA	Processo de Gestão do Risco de Segurança da Informação
Plan	• Definição do contexto • Processo de avaliação do risco • Preparação do plano de tratamento do risco • Aceitação do risco
Do	• Implementação do plano de tratamento do risco
Check	• Monitorização e análise crítica do risco
Act	• Manutenção e melhoria do processo de Gestão do Risco de Segurança da Informação

Para evidência perante processos de auditoria e para verificação, a qualquer altura, dos resultados obtidos em cada etapa do processo de gestão do risco, estes devem ser documentados, na íntegra e de forma detalhada.

A eliminação total e permanente do risco é um cenário utópico para as empresas, daí que a gestão do risco e as opções de tratamento adotadas visem, acima de tudo, assegurar que o risco aceitável é-o a um custo também aceitável tendo em conta a realidade da empresa.

No ponto seguinte é abordada e desenvolvida a Declaração de Aplicabilidade, documento fundamental para o estabelecimento do SGSI, na medida em que define como será implementada a segurança da informação.

4.1.7. Declaração de Aplicabilidade

Elaborado o Plano de Tratamento do Risco, este documento obrigatório apenas identifica os controlos associados à identificação, análise e avaliação de risco realizadas.

As exigências de segurança das empresas incidem, no entanto, também sobre outros processos, aspetos legais ou até áreas específicas que requerem controlos que vão além do tratamento a aplicar aos riscos. Por estes motivos, a norma NP ISO/IEC 27001:2013 impõe a produção de outro *output* fundamental: a **Declaração de Aplicabilidade.**

A **Declaração de Aplicabilidade** tem como finalidade indicar quais os controlos aplicáveis à empresa, se estes já estão aplicados ou não, a forma como foram implementados e os motivos para a sua inclusão assim como para eventuais exclusões. Todos os controlos genéricos que compõem o Anexo A da norma NP ISO/IEC 27001:2013 compõem também esta Declaração, podendo, no entanto, ser definidos controlos específicos. A descrição da implementação dos controlos pode mencionar, por exemplo, a política aplicada ou o procedimento utilizado.

A relação entre a Declaração e o Plano de Tratamento do Risco ocorre na medida em que na Declaração devem ser assinalados os riscos que estão sendo tratados e indicada a documentação relacionada com a aplicação dos controlos selecionados.

Na Declaração de Aplicabilidade verifica-se uma clara distinção entre os termos "Não Aplicado" e "Não Aplicável", sendo "Não Aplicado" todo e qualquer controlo cuja exclusão foi decidida por não existir risco associado que o justificasse, por ser "Não aplicável" ou por se verificar alguma sobreposição de controlos.

É de realçar que, num cenário de certificação ISO 27001, a Declaração de Aplicabilidade é o documento solicitado e utilizado pelos auditores aquando da observação das boas práticas implementadas na empresa. É a partir dos controlos aqui definidos que é verificada a sua efetiva implementação de acordo com a descrição realizada.

Além de ser um artefacto primordial para efeitos de certificação, a produção da Declaração de Aplicabilidade resulta num documento que demonstra o perfil de segurança da empresa, facultando aos administradores, gestores e técnicos uma visão global do que é necessário fazer, por que motivo tem de ser feito e como deverá ser feito.

No Anexo VIII consta uma proposta de Declaração de Aplicabilidade para a IHM, referente às secções da norma que compõem o âmbito do SGSI neste trabalho (secções A.5, A.12, A.13 e A.16). Elaborado este documento, concluiu-se a fase inicial de planeamento do SGSI com base na norma NP ISO/IEC 27001:2013.

Em seguida é abordada a Gestão de Incidentes, caraterizada por um conjunto de processos recomendados pelo *National Institute of Standards and Technology* (NIST), que se optou por integrar no diagrama de processos da norma NP ISO/IEC 27001:2013 apresentado na ***Figura 9***, por se relacionar com a secção A.16 - Gestão de incidentes de segurança da informação, a ser implementada.

4.1.8. Gestão de Incidentes

Esta componente reflete o ciclo de vida da resposta a incidentes da norma SP 800-61r2 do *National Institute of Standards and Technology* (NIST) e contém processos para detetar, analisar, conter, erradicar e recuperar de incidentes, assim como outras atividades pós-incidente.

Sendo um alvo apetecível para os atacantes pela informação que possuem, é expectável que toda e qualquer empresa venha a ser alvo de algum tipo de incidente de segurança, com maior ou menor impacto e frequência. Este pressuposto revela uma necessidade incontornável que é a empresa dispor de processos que lhe permitam estar preparada para gerir todo o ciclo de vida dos incidentes, como preconiza a NIST SP 800-61r2.

A deteção de incidentes obriga à observação dos eventos de segurança, ou seja, dos dados relacionados com os sistemas. Quando estes revelam ter ocorrido uma violação da segurança, ou a existência dessa possibilidade, então estamos perante um incidente de segurança. Para lidar com um incidente, a empresa deve ser capaz de identificar, reagir e recuperar da sua ocorrência, o que é facilitado com a existência de uma *Computer Emergency Response Team* (CERT). CERT é uma equipa especializada e treinada para monitorizar, identificar e responder a incidentes de segurança através de um plano estabelecido para controlar os custos e danos associados a incidentes, e para otimizar a recuperação de sistemas afetados.

Em cenários onde não há qualquer planeamento para a gestão de incidentes, a ocorrência de um incidente resulta, normalmente, na total atenção dada à resolução do problema, sendo deixado para segundo plano, ou até negligenciado, o registo documental das ações realizadas e os resultados obtidos, que poderão ser solicitados para efeitos legais. Adicionalmente, não é suposto que um especialista de segurança se recorde de todos os detalhes sobre uma ocorrência no passado, pelo que o registo detalhado dos incidentes é um dos processos fundamentais da gestão de incidentes.

PREPARAÇÃO

A preparação para a ocorrência de incidentes requer a realização de um conjunto de procedimentos importantes. A empresa deverá estabelecer uma política para a resposta a incidentes que abranja todos os procedimentos desde a deteção do incidente e defina as responsabilidades, os canais de comunicação, a recolha de evidências e o registo documental.

A CERT ou os especialistas em segurança, caso a empresa não disponha de recursos suficientes para a constituição de uma CERT, devem dispor de *hardware* e *software* adequado e receber formação contínua, de forma a estarem atualizados e melhor preparados para lidar com as ameaças mais recentes. Os planos de formação devem incluir a realização de testes em ambiente controlado, que reflitam cenários de ataque reais. Exercícios de simulação que envolvam toda a organização devem ser devidamente identificados para evitar qualquer

disrupção nos serviços. A realização destes exercícios é fundamental para avaliar a maturidade da empresa perante um cenário de incidente, para identificar pontos de falha e para desencadear processos de melhoria.

A preparação inclui igualmente a elaboração de uma *checklist* com as ações a realizar nos processos seguintes, para que os especialistas saibam exatamente o que fazer e em que ordem o devem fazer. A NIST SP 800-61r2 propõe uma *checklist* com tais ações, como são exemplo as apresentadas na Tabela 10. Por cobrirem o ciclo de vida da gestão de incidentes, considerou-se muito útil a adoção dos procedimentos identificados, que, no entanto, podem ser complementados com mais detalhe.

Particularmente em relação aos precursores e indicadores, a NIST SP 800-61r2 clarifica os termos: "um precursor é um sinal de que um incidente pode ocorrer no futuro. Um indicador é um sinal de que um incidente pode ter ocorrido ou pode estar ocorrendo agora" [56, p. 26].

Daqui se deduz que se forem detetados precursores, a empresa pode conseguir evitar o incidente efetuando as alterações necessárias às suas definições de segurança para protegerem um alvo de um ataque. Um exemplo de precursor é o anúncio de uma ameaça que tem como alvo explorar uma vulnerabilidade que possa estar presente num dos servidores da empresa. Já os *logs* de uma aplicação indicarem múltiplas tentativas de login falhadas a partir de um sistema remoto desconhecido é um exemplo de indicador de uma tentativa de ataque.

No Anexo XI apresenta-se a *checklist* completa de ações recomendadas pela NIST SP 800-61r2.

Tabela 10 - Checklist de ações para a gestão de incidentes (exemplo para a fase de deteção e análise)

	Ação
	Deteção e Análise
1.	Determinar se ocorreu um incidente
1.1	Analisar precursores e indicadores
1.2	Procurar informação correlacionada
1.3	Pesquisar e investigar (e.g. motores de busca, *knowledge base*)
1.4	Assim que seja crível que ocorreu um incidente, iniciar a documentação da investigação e a recolha de evidências
2.	Estabelecer prioridades para lidar com o incidente, de acordo com fatores relevantes (e.g. impacto funcional, impacto na informação, esforço de recuperação)

DETEÇÃO E ANÁLISE

Nem todos os eventos de segurança resultam de ataques aos sistemas de informação. Os eventos de segurança podem estar relacionados com vulnerabilidades identificadas que

aumentam o risco de ameaça ou com outras ações nos sistemas, cujos automatismos as registam, identificam e classificam.

A deteção e análise de eventos de segurança é a fase do ciclo que requer capacidade de investigação para determinar quais os eventos que resultaram ou podem resultar em incidentes de segurança com efeitos nocivos para os sistemas e para a empresa. Tratando-se, por vezes, de milhares de eventos, a deteção de eventos suspeitos deve ser realizada com recurso a automatismos, tais como sistemas de deteção e prevenção de intrusões (IDPS) *host-based* e *network-based*, *software* antivírus e analisadores de registos (*logs*), o que ajuda os especialistas a lidar com as ocorrências em tempo aceitável.

CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

Identificado um incidente, inicia-se a fase de contenção, cujo objetivo é intervir nos sistemas afetados de forma a isolá-los e evitar a propagação a outros sistemas. Dependendo da gravidade do incidente, o isolamento pode ser feito ao nível da rede ou através da aplicação de outros controlos mais rígidos, como seja o corte de energia, salvaguardando, no entanto, a recolha de evidências.

Nesta etapa são realizadas imagens do sistema que permitem a análise forense. Antes de desligar o sistema da corrente elétrica é também fundamental obter a informação volátil, por exemplo os processos que estão a correr no sistema, pois nem sempre a prova reside nos discos. A decisão de desligar um sistema deve ser tomada superiormente, na medida em que causa impacto negativo imediato no negócio.

A erradicação, ou mitigação, de um incidente exige o conhecimento da sua causa para evitar que o sistema se mantenha comprometido ou venha a sofrer um novo incidente pela mesma razão. Um exemplo de determinação da causa de um incidente é considerar que a ocorrência de *malware* num sistema é um sintoma e não a própria causa, ou seja, que existe uma vulnerabilidade que permitiu a entrada do *malware* no sistema.

As atividades de remediação executadas para eliminar as vulnerabilidades não terminam, contudo, na etapa de mitigação, devendo ser executadas em maior profundidade assim que ocorra a estabilização do sistema. Por exemplo, a alteração de uma palavra-passe comprometida pode dar lugar a que, mais tarde, se proceda à implementação de mecanismos de autenticação dupla (*dual-factor*).

O restauro de um sistema pode ser feito com recurso a um *backup* bem realizado ou, em última instância, implicar a reinstalação de todo o *software* e a realização de todas as parametrizações do sistema, o que envolve um tempo de recuperação bastante mais elevado e com certeza não aceitável pela empresa. A reposição de um *backup* considerado "bom" requer, contudo, alguns cuidados pois é necessário ter a certeza que este não foi comprometido pela ocorrência do incidente antes da sua deteção.

Daqui se conclui a necessidade dar credibilidade às decisões a tomar, nomeadamente a de reposição de um *backup*, o que pode ser conseguido com a identificação de eventos através de

uma linha de tempo. Recuperado o sistema, é fundamental reforçar a defesa do mesmo, seja através da aplicação de *patches* de segurança, seja pela imposição de mais restrições na *firewall* do sistema, e monitorizá-lo para assegurar que a erradicação da ameaça foi bem concretizada.

REPORTE

O reporte de um incidente de segurança de informação não representa uma fase do ciclo de vida da gestão de incidentes em particular, por ser um processo transversal a partir do momento da deteção. O reporte deve ser realizado em duas vertentes: o reporte técnico, que inclui detalhes da ocorrência e das ações realizadas, deve ser produzido pelos membros da CERT à medida que lidam com o incidente, e permite à equipa manter-se atualizada. Perante incidentes graves que afetam o funcionamento da empresa, deve ser estabelecido e mantido um canal de comunicação adequado com a Administração e com as autoridades adequadas, no sentido de notificá-las e mantê-las atualizadas sobre o desenvolvimento das ações. Assim que a situação se encontre controlada e os sistemas estejam em vias de retomar a produção, devem ser produzidos os reportes formais às referidas entidades.

ATIVIDADES PÓS-INCIDENTE

As atividades pós-incidente constituem a fase de maior potencial para a CERT, por poder resultar em mudanças positivas nos procedimentos e na postura adotada até então. Nesta etapa é elaborado o relatório final a ser apresentado à Administração da empresa. Além de mencionar os factos ocorridos, este deve conter considerações sobre como a identificação do incidente poderia ter ocorrido mais cedo, como a resposta poderia ter sido mais célere ou eficaz, quais os aspetos organizacionais que podem ter contribuído para o incidente e quais a áreas que podem ser melhoradas.

A informação a prestar no relatório deve ser clara e detalhada quanto às medidas técnicas e administrativas que podem melhorar a capacidade de deteção, contenção, erradicação ou recuperação de um incidente. As lições aprendidas e reconhecidas nesta fase são fundamentais para melhorar a preparação para incidentes futuros.

ANÁLISE FORENSE

A análise forense relaciona-se de forma muito próxima com a resposta a incidentes de segurança na medida em que aborda a investigação e a prova de um ponto de vista formal, ou seja, tendo em conta os aspetos legais do processo numa perspetiva criminal.

Para a realização de análise forense é necessário preservar o cenário do crime e as provas para que seja mantida a sua integridade. Durante muito tempo assumiu-se como fundamental para preservação da integridade da informação nos sistemas desligar a fonte de energia do equipamento. No entanto, esta abordagem falha perante um ataque em que, por exemplo, o

malware não resida nos discos, mas sim na memória volátil, como é o caso da memória RAM. Desligar o sistema significa destruir a prova do ataque.

Para não perder o valor da informação existente na memória volátil, as técnicas de análise forense são muitas vezes realizadas *live*, isto é, com o sistema em pleno funcionamento, se bem que isolado para evitar a contaminação de outros sistemas, sendo efetuada a recolha de informação sobre os processos ativos no sistema.

O processo forense consiste em identificar uma potencial prova, obter essa prova, analisá-la e produzir o relatório que detalha a prova obtida. A obtenção da prova é feita com recurso a *backups* e a algoritmos *hash* para verificar a integridade dos dados. A análise não deve ser feita sobre os media originais, mas sim aos *backups* e também a discos rígidos e dispositivos de armazenamento amovíveis (drives USB, smartphones, *players* mp3/mp4, CDs e DVDs).

É importante realçar que nos *backups* ditos normais, são copiados dados de espaço em disco que se encontra alocado, normalmente ficheiros e pastas. No entanto, o espaço não alocado (e.g. *slack* num *cluster* ou bloco de dados; ou um *bad block*) pode ser usado pelo atacante para esconder a evidência do ataque, no que se denomina de técnica anti-forense.

Quando realizada na rede, a análise forense tem como foco a informação em movimento. A legalidade da recolha, assim como a integridade, é fundamental para fazer prova em tribunal. Este tipo de análise tem muito a ver com a deteção de intrusões na rede, pois as provas muitas vezes não residem nos sistemas, mas sim nas redes. A análise forense na rede permite recuperar conteúdos de *e-mails*, conversas em *chats*, atividades de navegação na *Web* e transferência de ficheiros para reconstrução até ser obtida a transação original. O foco desta análise é verificar o envelope que carrega a informação e não apenas a informação, pelo que o protocolo de rede utilizado é muito importante para o investigador.

Ao longo deste trabalho foi possível testemunhar a ocorrência de um incidente de segurança de informação na Investimentos Habitacionais da Madeira (IHM), que embora tratado e ultrapassado com sucesso, veio confirmar as carências já identificadas como parte do problema a ser resolvido através de um sistema de gestão de segurança da informação (SGSI), nomeadamente a nível dos processos de planeamento.

Não sendo possível, por motivos de confidencialidade, especificar tal incidente, importa, no entanto, evidenciar que do mesmo resultou uma maior consciência para a importância da segurança da informação, assim como novos desafios ao nível da comunicação, da recolha de evidências, do envolvimento de todos os membros da equipa técnica e da atribuição de responsabilidades, sendo premente implementar os mecanismos em falta e melhorar os processos de gestão de incidentes abordados neste capítulo.

4.1.9. Revisão e Auditoria

Segue-se neste trabalho a fase de implementação do SGSI, que se apresenta de forma detalhada no próximo capítulo. Não sendo possível, no espaço temporal disponível aguardar largos meses até que seja viável a realização de uma revisão global do SGSI, a que

correspondem no Diagrama de Processos da ***Figura 9*** (Anexo III) os processos *12 – Revisão da Conformidade*, *13 – Medidas Corretivas* e *14 – Pré-avaliação de certificação*, optou-se por simplificar esta parte da análise desses processos, assim como do processo *15 – Auditoria de Certificação*, com uma breve descrição e mencionando os passos a realizar.

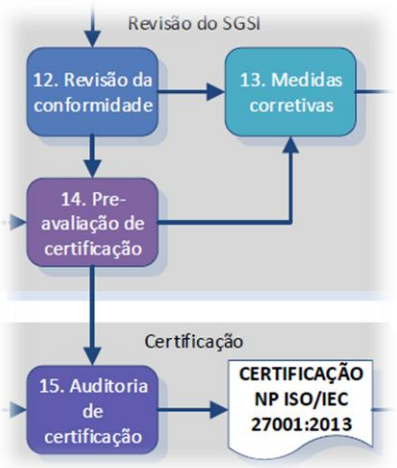


Figura 14 – Extrato dos processos para revisão do SGSI e para certificação no Diagrama de Processos

A revisão da conformidade corresponde à fase *Check* do ciclo PDCA que consiste em avaliar os indicadores de desempenho dos controlos aplicados, confrontando-os com a política do SGSI. Atendendo à natureza evolutiva dos sistemas, ao aumento do número de ataques, às técnicas de intrusão cada vez mais sofisticadas e à necessidade de critérios de segurança cada vez mais apertados, os resultados desta avaliação cíclica impõem uma análise crítica e a revisão da política, quando aplicável. As medições a realizar referidas no capítulo 5 são um primeiro indicador acerca da conformidade e da necessidade dessa revisão. Se as medições aos controlos aplicados não atingirem valores próximos do expectável, então será necessário aplicar medidas corretivas.

A aplicação de medidas corretivas perfaz o ciclo completo PDCA. Nesta fase *Act* são realizadas ações de melhoria aos controlos cujos indicadores de desempenho, como referido, não apresentaram resultados satisfatórios. Tais ações poderão ser a aplicação de melhor tecnologia, redefinição de acessos, otimização das tarefas, redefinição de responsabilidades, entre outras. É nesta fase que se concretiza a melhoria contínua do SGSI.

O processo de pré-avaliação de certificação é um processo de planeamento no qual são determinados todos os requisitos para a realização de uma auditoria de certificação e avaliada a sua viabilidade face ao nível de maturidade dos processos atingido pela empresa. Tratando-se, neste caso, de um processo de auditoria de segurança, este consiste num teste aos requisitos da norma NP ISO 27001:2013, em que o auditor verificará se a empresa cumpre com a norma publicada.

4.2. CONCLUSÕES

Em resumo, a metodologia proposta para a resolução do problema baseia-se na norma NP ISO 27001:2013 e passa pela aplicação de uma série de processos de planeamento, implementação, avaliação e correção, cujo objetivo principal é avaliar o risco de segurança associado aos bens inventariados, tendo em vista a aplicação de controlos de segurança adequados à mitigação desses riscos. Tratando-se de um processo cíclico, os controlos implementados são medidos, impondo-se a sua correção e melhoria caso não correspondam ao nível de segurança esperado. Atendendo a que este trabalho decorre em paralelo com o normal funcionamento da empresa e que ameaças à segurança podem surgir a qualquer momento, analisou-se também o conjunto de processos de gestão de incidentes da noma NIST SP 800-61r2, fundamentais para que a IHM esteja preparada para lidar com esta eventualidade.

Em seguida, inicia-se a segunda fase do ciclo PDCA respeitante à implementação do SGSI, que arranca com o desenvolvimento do programa de implementação do SGSI.

5. IMPLEMENTAÇÃO DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Nos capítulos anteriores identificou-se o problema, em concreto a insuficiência de processos para reforço da segurança da informação na empresa Investimentos Habitacionais da Madeira (IHM), tendo-se apresentado uma análise e metodologia para a sua resolução. Optou-se pela norma NP ISO 27001:2013 que especifica os requisitos para "estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação" (SGSI) [18, p. 6], por ser o padrão de referência desenvolvida especificamente para a aplicação de controlos de segurança da informação.

Atendendo à extensão da norma, composta por 14 secções e mais de uma centena de controlos genéricos, decidiu-se restringir a seleção a quatro dessas secções, as que se considerou mais relevantes para o contexto atual da IHM. Para o efeito, adotou-se um conjunto de processos que seguem o ciclo *Plan – Do – Check – Act* (PDCA). Sendo que uma das secções escolhidas tem como foco a gestão de incidentes, integrou-se na metodologia proposta a norma NIST SP 800-62r2, específica para esta temática.

Especificados os processos da fase de planeamento do SGSI, produzidos os *outputs* Plano de Tratamento do Risco e Declaração de Aplicabilidade, e abordados os processos de gestão de incidentes, prosseguiu-se com o início do processo de desenvolvimento do programa de implementação do SGSI para a IHM. Este processo, o primeiro da fase "*Do*" do ciclo PDCA, incide sobre os aspetos de suporte e de operação explanados nas cláusulas 7 e 8 da norma NP ISO 27001:2013, respetivamente.

A referida cláusula 7, sobre o suporte, indica que a organização deve proporcionar os recursos necessários ao SGSI, assegurar a competência das pessoas nele envolvidas, consciencializar os colaboradores da política de segurança implementada, determinar a necessidade para as comunicações internas e externas incluindo os processos pelos quais deve ser efetuada e assegurar que a informação documentada é controlada em termos de distribuição, acesso, armazenamento, controlo de versões e eliminação. Já a cláusula 8, sobre a operação, estabelece que a organização deve assegurar o controlo operacional, realizar avaliações do risco em intervalos planeados ou quando ocorrem alterações significativas e manter um plano de tratamento do risco [18, pp. 10–12].

A implementação do SGSI assume a realização prévia do inventário de ativos, a disponibilidade dos resultados da avaliação do risco, o tratamento a aplicar e os controlos a implementar, elementos resultantes do trabalho realizado nos capítulos anteriores. Adicionalmente, requer a definição das funções na gestão da segurança da informação, nomeadamente o estabelecimento de papéis e responsabilidades, tarefa já realizada e apresentada no Anexo V.

No seguimento do desenvolvimento do **Programa de Implementação do SGSI**, definiu-se um plano para cada secção da norma. Esta abordagem corresponde ao processo 11 do Diagrama

de Processos, ilustrado na ***Figura 9*** e em plano maior no Anexo III, tendo-se considerado cada secção como um projeto.

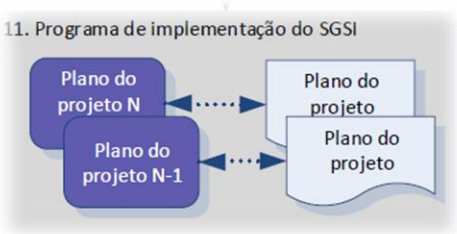


Figura 15 – Processo 11. Programa de implementação do SGSI no Diagrama de Processos

Nos subcapítulos seguintes são detalhados os aspetos de segurança e os controlos mais importantes para cada uma das secções escolhidas.

Na **secção A.5** - *Políticas de segurança de informação*, cujos controlos passam pela criação de políticas para a segurança da informação, a instalação de *software*, a realização de cópias de segurança, a utilização de correio eletrónico, entre outras, e respetiva revisão periódica, o objetivo é diminuir a probabilidade de ocorrência de incidentes pelo facto de a política ser o documento que permite a imposição de regras de segurança.

A **secção A.12** - *Segurança de operações*, com controlos para a melhoria de operações sobre os recursos de informação, tais como a documentação de procedimentos, a gestão de alterações, a gestão da capacidade, a aplicação de princípios de segurança, entre outros, tem como objetivo assegurar que os procedimentos são realizados de forma correta e segura

A **secção A.13** - *Segurança de comunicações*, com controlos a nível de *firewall*, gestão dos equipamentos ativos de rede, atualizações de *firmware*, serviços de rede, mensagens eletrónicas e também de acordos de confidencialidade e de não divulgação, entre outros, visa atender às necessidades de proteção da informação em circulação na rede LAN e nas VPN da empresa.

Na **secção A.16** - *Gestão de incidentes de segurança da informação,* cujos controlos incluem a definição de papéis, a ordem de intervenção durante uma ocorrência, o registo do número de incidentes, a aplicação do plano de resposta em caso de ocorrência, entre outros, pretende-se atender à preparação, deteção, análise, contenção, erradicação, recuperação e reporte de incidentes, assim como à recolha de evidência, tendo também como objetivo a obtenção de conhecimento para melhoria em ocorrências futuras.

A lista completa de controlos para as quatro secções é apresentada no Anexo IX. De referir que a cada controlo corresponde uma série de atributos de informação estabelecidos na norma ISO/IEC 27004:2016 [21, p. 26], que são úteis por indicarem os aspetos da medição em foco nesta fase. Em concreto, para cada controlo são indicados:

- **ID da medição**, que é uma identificação a definir internamente na empresa;
- **Necessidade de informação**, ou seja, a razão pela qual se mede o controlo;

- **Medida**, que quantifica a medição efetuada;
- **Fórmula**, que estabelece o cálculo;
- **Alvo**, que corresponde à escala ou valor que se pretende atingir;
- **Evidência de implementação**, que corresponde à prova de que o controlo é executado;
- **Frequência**, que indica a o critério ou a periodicidade da recolha, análise e reporte de medições ou outras ações realizadas;
- **Partes responsáveis**, que indica as entidades com responsabilidades no controlo;
- **Fonte de dados**, que suporta a realização do controlo;
- **Formato de reporte**, que estabelece a forma de apresentação dos resultados obtidos.

5.1. PLANO DA SECÇÃO A.5 – POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Considerando-se as atividades já realizadas nos processos anteriores, definiu-se em seguida a estrutura da política de segurança atendendo às recomendações presentes no Anexo D da norma auxiliar ISO/IEC 27003:2010 [20, p. 57]. Pela importância deste instrumento para a segurança da informação, transcreve-se a definição e os conceitos apresentados no referido anexo D:

"Em geral, uma política é uma declaração de intenção e de direção expressa formalmente pela administração. O conteúdo de uma política orienta as ações e decisões relativas ao tema da política. Uma organização pode ter várias políticas, uma para cada uma das áreas de atividade que é importante para a organização. Algumas políticas são independentes umas das outras, enquanto outras políticas têm uma relação hierárquica. Na área da segurança, as políticas são geralmente organizadas hierarquicamente. Normalmente, a política de segurança da organização é a política de nível mais elevado. Esta é suportada por um conjunto de políticas mais específicas, incluindo a política de segurança da informação e a política do Sistema de Gestão de Segurança da Informação. Por sua vez, a política de segurança da informação pode ser apoiada por uma série de políticas mais detalhadas sobre tópicos específicos relacionados com aspetos da segurança da informação" [20, p. 57].

Atendendo ao acima exposto, e considerando que a norma NP ISO/IEC 27001:2013 refere genericamente o estabelecimento de políticas de segurança da informação, decidiu-se que o estabelecimento desta política fosse concretizado e complementado com políticas específicas, tais como as políticas para a instalação de *software*, a realização de cópias de segurança, a utilização de correio eletrónico, entre outras. Crê-se que esta opção facilita o entendimento das regras estabelecidas, assim como a sua atualização sempre que necessário.

Em termos de estrutura, optou-se por adaptar o proposto na norma ISO/IEC 27003:2010 [20, p. 58], nomeadamente definir a estrutura das políticas com os seguintes elementos:

1. Resumo – uma breve explicação sobre o tema da política.
2. Objetivos – descrição da intenção da política.
3. Âmbito – descrição dos elementos ou atividades da empresa abrangidos pela política.
4. Política – descrição das regras referentes às ações e decisões para atingir os objetivos.
5. Responsabilidades – descrição de quem é responsável pelas ações para que os requisitos da política sejam cumpridos.
6. Histórico de revisões – informação sobre a edição, aprovação, versão, estado e validade da política.

No seguimento do exposto anteriormente sobre a política de segurança da informação, esta é um elemento fundamental para a governança da segurança da informação na medida em que a sua não existência resulta na falta de regras para fazer cumprir e, consequentemente, na perda de substância da própria governança.

Neste âmbito, o *National Institute for Standards and Technology* (NIST), apresenta também uma definição importante que complementa a definição apresentada pela ISO/IEC 27003:2010 [20, p. 57]: "a política de segurança da informação é um agregado de diretivas, regras e práticas que determina como uma organização gere, protege e distribui informação" [64, p. 14].

Para gerir, proteger e distribuir adequadamente a informação é necessário que a política de segurança da informação se mantenha atual e relevante, pelo que revisões periódicas devem ser executadas sob pena de um aumento do risco de segurança por obsolescência da informação conhecida. A revisão e melhoria dos controlos aplicados deve seguir a revisão da política, com conhecimento aos intervenientes, nomeadamente aos colaboradores e aos prestadores de serviços, quando aplicável.

O plano desta secção consistiu na identificação de um conjunto de políticas que se considerou relevantes para a IHM e que totalizam 21 controlos, número superior ao do Anexo A da norma NP ISO/IEC 27001:2013 que apenas contém 2 controlos genéricos. O motivo, como mencionado, prendeu-se com a opção por políticas específicas ao invés de uma política única que se previu tornar-se demasiado longa, densa e de mais difícil leitura. Apresenta-se, assim, uma descrição sucinta de cada uma dessas políticas, destacando-se e sublinhando-se as produzidas neste trabalho e categorizando por destinatário:

POLÍTICAS PARA TODOS OS UTILIZADORES

Política de Segurança da Informação – estabelece as regras gerais e os princípios para a segurança da informação, seja qual for o seu formato, a forma como é partilhada, comunicada

ou armazenada, de modo a garantir a continuidade do negócio e a minimizar os riscos resultantes de ameaças físicas e lógicas.

Política de Correio Eletrónico – define as regras para a utilização do sistema de *e-mail* da IHM, de contas do domínio ihm.pt e informa a utilização que a IHM considera aceitável e inaceitável deste sistema.

Política de Palavra-passe – define os requisitos para a definição de palavra-passe complexa de acesso ao domínio e aplicações, para utilizadores e administradores, a ser renovada periodicamente.

Política de Gestão de Incidentes de Segurança da Informação – estabelece os procedimentos desde a deteção do incidente e define as responsabilidades, os canais de comunicação, a recolha de evidências e o registo documental.

E ainda, a estabelecer futuramente:

Política de Classificação da Informação, que especifica a classificação a atribuir à informação digital produzida (e.g. pública, restrita ou confidencial).

Política de Dispositivos Móveis (incluindo *Bring Your Own Device* (BYOD)), que especifica a utilização de portáteis, *tablets*, smartphones e outros dispositivos móveis, incluindo BYOD, para tratamento de dados da IHM.

Política de Navegação na Web, que especifica o acesso a *Web* sites e a conteúdos descarregáveis.

Política de Teletrabalho, que especifica as regras de acesso remoto aos recursos informáticos da empresa.

Política de Utilização de Redes Sociais, que especifica as regras para partilha de conteúdos proprietários da empresa, resposta a clientes e comentários de natureza profissional.

POLÍTICAS ESPECÍFICAS PARA TÉCNICOS DE INFORMÁTICA

Política de Instalação de Software – define os requisitos para instalação de *software* nos sistemas de produção da empresa. Pretende-se minimizar o risco de infeção dos sistemas, o risco de perda de informação e de funcionalidades nos programas e o risco de incumprimento legal por utilização de *software* não licenciado.

Política de Cópia de Segurança – define as regras para a realização de *backups* de dados, dos controladores de domínio, criação de imagens dos sistemas aplicacionais, verificação da sua integridade e testes de reposição para garantia da disponibilidade em caso de incidente e minimização do tempo de recuperação.

Política de Segurança de Rede – define a utilização aceitável da rede de dados e as regras para a segurança da infraestrutura e perímetro da rede.

Política de Transferência de Informação – define as regras para a transferência segura de dados entre sistemas internos e servidores, bem como de informações para entidades externas através da rede.

E ainda, a estabelecer no futuro:

Política de Segurança Física, que especifica os controlos de acesso físico às instalações e os mecanismos de proteção dos recursos físicos.

Política de Controlo de Acesso, que especifica as regras de acesso aos sistemas, o registo de utilizadores e a gestão de direitos de acesso.

Política de Encriptação de Dados, que especifica a utilização de mecanismos de encriptação para salvaguarda da confidencialidade e integridade da informação transmitida e armazenada.

Política de Desenvolvimento Aplicacional, que especifica as regras para o desenvolvimento seguro de *software*, as linguagens e metodologias a adotar, o controlo de versões, os testes de segurança e de aceitação e a documentação a produzir.

Optou-se por produzir nesta fase do trabalho a política de segurança da informação, a política de instalação de *software*, a política de cópia de segurança (*backups*) e a política de correio eletrónico por já existirem procedimentos relacionados implementados na empresa, mas que requerem revisão para diminuição do risco de segurança.

Por imposição legal, a política de palavra-passe existente foi ajustada para conformidade com os requisitos técnicos mínimos das redes e sistemas para aplicação do RGPD [65]. Remete-se para trabalho futuro o desenvolvimento das restantes políticas, salientando-se a importância de todas para a redução dos riscos de segurança.

Na Tabela 11 apresenta-se um dos controlos definidos para esta secção (controlo A.5.1.1) e os atributos de informação que permitem a realização de uma medição do controlo, neste caso medir o n.º de políticas estabelecidas por ano.

Tabela 11 - Controlo a implementar para a secção A.5 (exemplo)

Controlo	A.5.1.1 – Políticas para a segurança da informação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se as políticas de segurança da informação necessárias são estabelecidas.
Medida	Percentagem de políticas estabelecidas.
Fórmula/Pontuação	(N.º de políticas de segurança de informação estabelecidas no último ano/Total de políticas de segurança da informação a estabelecer) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%

Alvo	Verde
Evidência de implementação	Documento que estabelece a política.
Frequência	Recolha de medições: anual Relatório: um para cada medição
Partes responsáveis	CA: responsável pela informação e pela aprovação das políticas Chefia Informática: responsável pela medição
Fonte de dados	Plano de definição de políticas
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

5.2. PLANO DA SECÇÃO A.12 – SEGURANÇA DE OPERAÇÕES

A segurança de operações passa por garantir a implementação de controlos que impeçam que atos intencionais ou inadvertidos possam comprometer a confidencialidade, a integridade e a disponibilidade nos sistemas de produção. Esta implementação é absolutamente relevante considerando que a necessidade de acesso à informação ocorre não apenas internamente, por parte de colaboradores, mas também por entidades externas autorizadas, sejam estes prestadores de serviços, parceiros ou outros.

Genericamente foi seguido um conjunto de princípios de segurança relacionados com o acesso aos dados nos sistemas:

O **Princípio do Menor Privilégio (ou Acesso Mínimo Necessário)**, que estabelece que "as pessoas não têm mais do que o acesso estritamente necessário para o desempenho das suas funções" [13, p. 349].

A **Separação de Deveres,** que requer várias pessoas para completar transações críticas ou sensíveis. O objetivo é garantir que "para abusar do acesso a dados ou transações sensíveis uma pessoa precisa de convencer outra a participar na ação" [13, p. 349].

A **Rotatividade de Funções,** que "ajuda a mitigar o risco associado a um indivíduo possuir demasiados privilégios" [13, p. 350] pois requer que um colaborador não execute funções críticas sem interrupção e que estas não sejam apenas do seu conhecimento. Ajuda também a deter intenções de fraude.

A **Defesa em Profundidade**, que implica a existência de múltiplos níveis de defesa de modo a não permitir o acesso ao sistema mesmo que o atacante consiga ultrapassar a primeira barreira de segurança [66, p. 5].

Na IHM, atendendo à escassez de recursos humanos em variadas áreas, os princípios mencionados são apenas parcialmente cumpridos, pelo que se justifica a sua inclusão nesta implementação como objetivo de melhoria. De referir que no caso do serviço informático, o acesso privilegiado a funções críticas nos sistemas exige maior escrutínio e controlos mais rígidos, nomeadamente sobre as operações mais importantes.

Na prática, a segurança das operações requer a aplicação de um vasto conjunto de controlos enquadrados nos requisitos do anexo A da norma NP ISO/IEC 27001:2013, que em seguida se resumem sucintamente:

PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS

- **Disponibilizar documentação** – disponibilizar no site interno (Intranet) os manuais de utilização, de administração de sistemas e aplicações, de boas práticas e *checklists* de procedimentos de acordo com o perfil e função do colaborador.

- **Criar, modificar e eliminar contas** – criar e modificar conta de utilizador apenas após a receção de *e-mail* com justificação do serviço requisitante. Desativar conta de antigos colaboradores assim que deixem de exercer funções na empresa. Eliminar contas apenas após validação jurídica da não existência de obrigações contratuais (incluindo no âmbito do RGPD).

- **Reiniciar sistemas** – garantir a não existência de sessões ativas e a mínima perturbação dos serviços aquando do reinício de um sistema. Alertar os serviços que operam em locais remotos. Agendar, preferencialmente, o reinício dos sistemas para horário pós-laboral salvo situação urgente.

- **Garantir a continuidade dos serviços** – a exigência de disponibilidade operacional requer mecanismos de tolerância a falhas, salvaguarda de dados e redundância, tais como a realização de *backup*, a redundância de discos e de hardware e *clusters* de alta disponibilidade para aplicações críticas.

- **Configurar sistemas** – as configurações devem permitir as funcionalidades estritamente necessárias. Não é aceitável a utilização de configurações de fábrica, facilmente conhecidas dos atacantes. Serviços desnecessários devem ser desativados e programas suspeitos ou inúteis igualmente desinstalados.

- **Aplicar redundância aos sistemas**: as aplicações críticas devem ser suportadas por um *cluster* (conjunto de sistemas) de alta disponibilidade, que assegure o funcionamento das aplicações caso um dos sistemas falhe.

- **Aplicar redundância ao *hardware*** - deve ser assegurada para os componentes mais suscetíveis a falhas. São exemplo a dupla fonte de alimentação, a redundância de placas de rede e de discos.

- **Configurar tecnologia RAID** - os sistemas devem ser suportados por configurações *Redundant Array of Inexpensive Disks* (RAID), por exemplo o RAID 5 que utiliza o espaço equivalente a um disco para redundância através de bits de paridade, distribuídos alternadamente entre todos os discos do *array*. Caso um dos discos falhe, a controladora RAID calcula e recupera os dados contidos no disco danificado e permite que o sistema continue a funcionar mesmo sem esse disco.

- **Gerir alterações que afetem a segurança** - qualquer alteração proposta deve ser avaliada quanto ao risco, aos custos associados e testada em ambiente virtual. Exigir um plano de reversão de forma a ser possível repor o estado anterior do sistema. Comunicar aos serviços afetados o agendamento das alterações e produzir um relatório da execução.

- **Gerir a capacidade dos sistemas** - os sistemas devem ter sempre mais de 40% de capacidade em disco disponível nos seus recursos para que seja possível acautelar atempadamente qualquer necessidade de reforço e garantir a disponibilidade da informação.

- **Criar ambientes distintos** – o desenvolvimento deve ser realizado em ambiente partilhado, dotado de tecnologia de controlo de versões (e.g. *Git Lab*), mas restrito e apenas acessível aos programadores e gestor de projeto envolvidos. Os testes ao desenvolvimento devem ser realizados em ambiente virtual distinto. A entrada em produção apenas deve ocorrer após validação do código produzido.

- **Contratar *Service Level Agreement* (SLA)** - os sistemas críticos devem ser suportados por um contrato SLA com os fabricantes e prestadores de serviços para minimizar os tempos de recuperação dos sistemas e aplicações.

PROTEÇÃO CONTRA CÓDIGO MALICIOSO

- **Proteger os *endpoints*** – instalar antivírus, ativar a *firewall* e impor controlos para instalação de *software*, utilização de media amovíveis e encriptação dos dados como camadas adicionais de segurança. Os dispositivos móveis utilizados fora do perímetro da IHM e com possível ligação a redes Wi-Fi desprotegidas também têm de estar devidamente protegidos.

- **Promover ações de consciencialização** – utilizar o contato diário com os utilizadores para realizar ações pedagógicas sobre segurança e alerta contra código malicioso. Enviar *e-mails* de alerta periodicamente. Promover a consciencialização dos utilizadores no âmbito das atividades de *helpdesk*.

SALVAGUARDA DE DADOS

O tipo de *backup* a realizar é definido de acordo com os tempos de execução e de recuperação atendendo à sua criticidade:

Tabela 12 - Tipos de backup

Tipo de *backup*	Tempo de execução	Tempo de recuperação
Completo	Longo	Curto
Incremental	Curto	Longo
Diferencial	Médio	Médio/Longo

- **Efetuar *backup* dos controladores de domínio** – efetuar diariamente cópia que inclua o sistema, os ficheiros reservados, o estado do sistema e recuperação "bare metal".

- **Criar imagens dos sistemas aplicacionais** – imagens dos sistemas aplicacionais devem ser realizadas diariamente para NAS e *tape* com encriptação.

- **Efetuar *backup* de dados das aplicações** – o *backup* dos dados das aplicações deve ser realizado diariamente para NAS e *tape* com encriptação.

- **Efetuar *backup* de dados dos utilizadores** – o *backup* dos dados das aplicações deve ser realizado semanalmente para NAS e *tape* com encriptação.

- **Verificar integridade dos *backups* e imagens** - os *backups* e as imagens de sistema devem ser testados e repostos semanalmente em ambiente virtual para verificação da sua integridade.

REGISTO DE EVENTOS E MONITORIZAÇÃO

- **Analisar registos de eventos** – analisar semanalmente os *logs* de segurança, de sistema e das aplicações nos servidores.

- **Proteger as informações registadas** – apenas os administradores e operadores de sistema devem ter acesso aos *logs*.

- **Rever atividades dos administradores e operadores de sistema**: exportar e filtrar mensalmente os *logs* nos sistemas dos utilizadores com privilégios de administração e operação nos sistemas para análise das atividades realizadas.

- **Sincronizar os relógios** - os relógios de todos os sistemas devem ser sincronizados com o *Windows Time service* (W32Time) no domínio, pois este serviço utiliza os algoritmos do *Network Time Protocol* (NTP) para garantir que os relógios nos computadores em toda a rede sejam tão precisos quanto possível.

CONTROLO DE SOFTWARE EM SISTEMAS DE PRODUÇÃO

- **Instalar software licenciado** – apenas software licenciado deve ser instalado nos sistemas de produção, em conformidade com os requisitos do sistema.

GESTÃO DE VULNERABILIDADES TÉCNICAS

- **Aplicar de *patches* nos sistemas operativos** – por regra a aplicação deve ocorrer semanalmente e em função da gestão do risco, sendo automática para *patches* de segurança e com máxima prioridade em situações urgentes (e.g. *patch* excecional da Microsoft para o *ransomware* "*wannacry*").

- **Aplicar de *patches* nas aplicações** – devem ser testados em ambiente virtual antes da aplicação ao ambiente de produção. De referir que em aplicações *client-side*, onde ainda não há desmaterialização, esta aplicação resulta num consumo elevado de recursos.

- **Estimar a gravidade das vulnerabilidades** – utilizar a *Common Vulnerability Scoring System Calculator* (CVSS) [67], exemplificada no Anexo XII. A CVSS "permite identificar as principais características duma vulnerabilidade e produzir uma pontuação numérica que reflita a sua gravidade (…) para ajudar as organizações a avaliar e priorizar adequadamente os seus processos de gestão de vulnerabilidades" [68].

- **Instalar software** – instalar apenas o software necessário às tarefas do utilizador, em conformidade com a política definida.

CONTROLOS DE AUDITORIA

- **Minimizar impacto das auditorias** – as auditorias devem ser calendarizadas de modo a causar o menor impacto nas atividades dos serviços, não devendo ser conduzidas em dias de processamento intensivo (e.g. aquando da integração de pagamentos).

Em resumo, apresentou-se 28 controlos administrativos e técnicos, fundamentais à redução do risco associado às vulnerabilidades, nomeadamente as verificadas nas operações. Muitos dos controlos identificados já são aplicados na IHM, pelo que o plano de implementação consistiu primeiro em rever as configurações realizadas e em seguida complementar com controlos em falta. As medições a realizar permitem determinar a capacidade dos processos envolvidos.

A Tabela 13 apresenta um excerto do controlo A.12.1.3 para a gestão de capacidade.

Tabela 13 - Controlo a implementar para a secção A.12 (exemplo)

Controlo	A.12.1.3 – Gestão da capacidade
Medida	Percentagem de capacidade disponível em cada sistema.
Fórmula/Pontuação	(Capacidade disponível em cada sistema/Total de capacidade em cada sistema) *100 Vermelho < 40%; Laranja <= 60%; Verde > 60%
Alvo	>= 40%
Evidência de implementação	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

5.3. PLANO DA SECÇÃO A.13 – SEGURANÇA DE COMUNICAÇÕES

A segurança nas comunicações "tem como foco a confidencialidade, a integridade e a disponibilidade da informação em movimento [13, p. 219], sendo fundamental nos dias de hoje em que as tecnologias mais utilizadas funcionam em rede e a navegação na Internet, o comércio eletrónico e o acesso a programas e plataformas de serviços como o *homebanking*, entre muitos outros, requerem elevado nível da segurança.

A gestão das comunicações na rede local (LAN) da IHM passa por gerir os serviços de rede disponibilizados, as configurações nos equipamentos de suporte (e.g. *routers* e *switches*) e as ligações por *Virtual Private Network* (VPN) aos locais remotos onde a empresa opera. Como noutros domínios da segurança informática, a segurança nas comunicações exige uma implementação em profundidade, ou seja, a aplicação eficiente de múltiplos controlos de segurança que evitem o comprometimento da informação em caso de falha de um controlo.

Sabendo-se ser impossível garantir a não ocorrência de ataques, é, contudo, fundamental adotar este tipo de estratégia para uma eficiente gestão das comunicações e dos aspetos de segurança a serem mantidos, devendo-se, todavia, confrontar o custo e a complexidade da rede com o benefício obtido.

O Anexo A da norma NP ISO 27001:2013 define controlos genéricos para a presente secção, cujo objetivo é melhorar a proteção da informação na rede, nomeadamente nos recursos de processamento e durante a sua transferência, ocorra esta dentro da empresa ou para entidades externas. Para o contexto atual e futuro da IHM, propõe-se e descreve-se, sucintamente, um conjunto mais alargado de controlos que integram os conceitos apresentados no referido anexo A:

CONTROLOS DE REDE

- **Adquirir equipamentos de rede com gestão remota e centralizada**: fundamental para a definição de configurações, a imposição de restrições de segurança ao tráfego e monitorização.

- **Garantir redundância dos equipamentos críticos**: a necessidade imperiosa de comunicações com o exterior, via internet, com a garantia de aplicação de restrições de segurança exige redundância de equipamentos, como seja a *firewall*.

- **Verificar regras na *firewall***: as regras definidas na *firewall* devem ser as necessárias para assegurar a máxima segurança, devendo as regras obsoletas ser eliminadas para diminuição do nível de risco.

- **Implementar DMZ com *firewall* dupla**: esta arquitetura é fundamental para serviços *Web* residentes em servidores locais (e.g. servidor *Web*, servidor de correio eletrónico). Estes devem ser colocados entre duas *firewalls*: uma para proteção da rede interna e outra para proteção da ligação à internet.

- **Monitorizar o sistema de deteção e prevenção de intrusões (IDS/IPS):** fundamental para determinar quais as vulnerabilidades que as tentativas de intrusão estão a querer explorar (e.g. identificação da porta 53 num ataque *Denial of Service* (DoS)).

- **Atualizar *firmware***: monitorizar o lançamento de atualizações de *firmware* e aplicá-las a todos os equipamentos de rede.

- **Segmentar a rede**: para garantir a independência de serviços, reduzir o tráfego na rede física e a exposição ao risco evitando o acesso indevido a equipamentos críticos, por exemplo, através de serviços de assistência técnica remota por parte de entidades fornecedoras.

- **Isolar portas (*port isolation*)**: útil quando sistemas virtualizados suportados pelo mesmo *hypervisor* não têm necessidade de acesso direto entre si. Com o isolamento de uma porta garante-se que esta apenas comunica com o *uplink*, não podendo comunicar com outros recursos na mesma sub-rede.

- **Mapear IP - MAC *Address***: o registo estático visa impedir que o atacante interfira nas respostas ARP. Implica um esforço de gestão adicional por exigir configurações de IP manuais.

SEGURANÇA EM DISPOSITIVOS *WIRELESS*

- **Desabilitar *broadcast* do *Service Set Identifier* (SSID)**: medida preventiva para evitar ligações desnecessárias ao dispositivo. Para fazer a ligação o SSID oculto tem de ser inserido tal como configurado pelo administrador de rede, em vez de apenas escolhido

numa lista. Apesar de ser uma medida insuficiente, pois há *sniffers* que detetam o SSID, deve ainda assim ser implementada.

- **Utilizar WPA2 802.11i (*Robust Security Network*) em todos os *Access Points* (APs)**: permite a ligação de módulos de autenticação e alterações às cifras criptográficas à medida que vulnerabilidades são descobertas. Este protocolo utiliza os algoritmos criptográficos AES para a confidencialidade e *Counter Mode* para a integridade.

- **Desabilitar o serviço *auto-discovery* em dispositivos Bluetooth**: esta tecnologia utiliza uma cifra fraca (128-bit E0 *Symetric Stream Cypher*). A descoberta de dispositivos Bluetooth é feita através dos 48 bits do MAC *Address*, em que 24 são o OUI (*Organizationally Unique Identifier*) que é conhecido e aos restantes 24 é aplicada força bruta.

SEGURANÇA DE SERVIÇOS

- **Desabilitar serviços de rede desnecessários**: a existência de serviços de rede ativos que não são necessários são um potencial foco de insegurança. O protocolo IPv6 que vem ativado por *default* na maioria dos sistemas operativos é um exemplo. Todos os serviços de rede que não sejam necessários devem ser desativados.

- **Implementar *Domain Name System Security Extensions* (DNSSEC)**: este controlo garante que apenas pesquisas verificadas criptograficamente obtêm acesso aos registos DNS. A garantia de integridade e disponibilidade a respostas DNS ocorre através de encriptação de chave pública (criptografia assimétrica).

TRANSFERÊNCIA DE INFORMAÇÃO

- **Utilizar *Secure Shell* (SSH)**: o carregamento de ficheiros para a *cloud* e as ligações a outros organismos devem ser efetuados através de SSH (ou túnel VPN IPSec) para garantia de confidencialidade, integridade e disponibilidade. Não deve ser permitida qualquer ligação Telnet ou FTP por motivos de insegurança.

- **Utilizar certificados de segurança em correio eletrónico**: as mensagens de correio eletrónico devem ser assinadas digitalmente para garantia de autenticidade e encriptadas sempre que o seu conteúdo seja sensível ou confidencial.

- **Implementar HTTPS**: para que a transferência de dados se realize através de uma ligação encriptada onde é verificada a autenticidade do servidor e do cliente através de certificados digitais SSL/TLS, e a informação transmitida apenas seja visualizada por estes.

- **Acordos de confidencialidade**: os colaboradores, fornecedores e outras entidades com acesso a dados da empresa devem assinar acordos de confidencialidade e de não divulgação de informação.

Na Tabela 14 consta um resumo do controlo A.13.1.2 desta secção para a segurança de serviços de rede. Os restantes controlos são apresentados no Anexo IX.

Tabela 14 - Controlo a implementar para a secção A.13 (exemplo)

Controlo	A.13.1.2 – Segurança de serviços de rede (1 de 5)
Medida	Percentagem de serviços de rede não necessários
Fórmula/Pontuação	(N.º de serviços de rede não necessários/Total de serviços de rede) *100 Verde < 20%; Laranja <= 80%; Vermelho > 80%
Alvo	0%
Evidência de implementação	Inventário de serviços

5.4. PLANO DA SECÇÃO A.16 – GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A gestão de incidentes de segurança tem como objetivo preparar a IHM para o aumento das tentativas de ataque ao funcionamento da rede e dos sistemas de informação, assim como para lidar com eventuais ocorrências e consequente impacto. Estes sistemas podem tornar-se alvo de ações danosas deliberadas, destinadas a danificar ou a interromper a sua operação, impedindo o normal exercício das atividades, gerando perdas financeiras importantes, minando a confiança dos utilizadores e causando graves prejuízos à empresa.

Para esta secção definiu-se 11 controlos que se enquadram nos processos que compõem a norma NIST SP 800-61r2, anteriormente abordados no capítulo 4, que cobrem a gestão de incidentes desde a preparação até às atividades pós-incidente. De referir que a existência de um incidente de segurança verifica-se se houver eventos que indiquem que uma violação da postura de segurança da empresa ocorreu ou pode estar a ocorrer, seja esta violação um incumprimento básico de uma política ou uma exfiltração massiva de dados.

Descreve-se, sucintamente, em seguida, um conjunto de controlos selecionados:

PROCEDIMENTOS E RESPONSABILIDADES

- **Definir planos de resposta e de recuperação** – identificar para cada sistema e ativo de rede configurável os procedimentos de resposta e recuperação, tendo em consideração a necessidade de recolha de evidência.

- **Atribuir papéis e responsabilidades** – a indivíduos específicos habilitados a lidar com incidentes em computadores, servidores e na rede, que efetuem o rastreio e documentem todo o incidente.

- **Estabelecer contatos em rede** – partilha de informações entre especialistas e organismos para alavancagem do conhecimento coletivo, antecipação a incidentes em curso e receção de alertas sobre incidentes noutros organismos.

REPORTE DE EVENTOS

- **Definir os canais de comunicação** – telemóvel, telefone interno, *e-mail* e contato pessoal.

- **Definir ordem de intervenção nas comunicações** – comunicações dos técnicos por ordem hierárquica. Informações à comunicação social prestadas por elemento da administração ou gabinete de assessoria.

- **Criar modelo de notificação** – para que qualquer colaborador possa reportar a informação relevante sobre um incidente.

- **Reportar incidentes às partes envolvidas** – informar os técnicos, os responsáveis dos serviços envolvidos e a administração da empresa o mais rapidamente possível.

- **Notificar as autoridades** – notificar a Polícia Judiciária e o Centro Nacional de Cibersegurança, em cumprimento com a legislação em vigor.

REPORTE DE PONTOS FRACOS

- **Instruir para a deteção** – promover ações de consciencialização junto dos colaboradores para a deteção e reporte de pontos fracos de segurança da informação.

- **Promover treino técnico em ambiente controlado** – realizar exercícios controlados (simulações) para pontos fracos identificados e cenários de vulnerabilidade plausível destinados à equipa técnica.

AVALIAÇÃO E DECISÃO SOBRE EVENTOS

- **Classificar incidentes** – examinar os eventos reportados pelos colaboradores, prestadores de serviços e automaticamente pelo IDS/IPS, pelo antivírus e os presentes nos *logs* dos sistemas e decidir se estes são incidentes de segurança.

RESPOSTA A INCIDENTES

- **Utilizar *checklist* de procedimentos** – *checklist* com as etapas e ações a realizar para que os especialistas saibam exatamente o que fazer e em que ordem o devem fazer.

- **Documentar as atividades de resposta** – registar as respostas dadas no decorrer das etapas de resposta.

APRENDER COM OS INCIDENTES

- **Promover reunião para discussão sobre as intervenções realizadas** – convocar todos os envolvidos nos procedimentos técnicos e tomadas de decisão.

- **Elaborar relatório final** – incluir os atos ocorridos, o *timestamp* (data, hora e minuto) mais aproximado possível, a identificação do incidente, os recursos afetados, os resultados da atividade de remediação, considerações sobre como a resposta poderia ter sido mais célere ou eficaz, os aspetos organizacionais que podem ter contribuído para o incidente, as áreas que podem ser melhoradas e as lições aprendidas.

- **Rever e atualizar os procedimentos de resposta** – identificar as medidas técnicas e administrativas para melhoria da capacidade de deteção, contenção, erradicação e recuperação

RECOLHA DE EVIDÊNCIAS

- **Identificar, recolher e preservar evidência forense digital** – preparar a disponibilidade de *software* e *hardware* que garantam a integridade das evidências obtidas.

Tabela 15 - Controlo a implementar para a secção A.16 (exemplo)

Controlo	A.16.1.2 – Reportar eventos de segurança da informação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o reporte de incidentes de segurança
Medida	Número de incidentes reportados num ano
Fórmula/Pontuação	(N.º de incidentes de segurança reportados num ano /Total de incidentes de segurança num ano) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Documentos de reporte enviados
Frequência	Recolha de medições: anual

Partes responsáveis	Chefia Informática: responsável pelo registo de incidentes e pela medição do controlo
Fonte de dados	Registo anual de incidentes
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

5.5. ANÁLISE CRÍTICA

As secções constantes do Programa de Implementação do SGSI apresentado no Anexo IX contemplaram a implementação de 47 controlos, tendo sido possível realizar a medição a 37 desses controlos ao longo de 30 dias, com recurso à aplicação da fórmula/pontuação definida para cada controlo. Por motivos de confidencialidade e segurança, a apresentação dos resultados no Anexo XIII é feita maioritariamente em percentagem.

Atendendo à dimensão variável de cada controlo, a recolha de informação foi célere em alguns casos, como por exemplo o controlo da secção A.12.1.4, sobre a percentagem de ambientes, por aplicação, isto devido ao pouco desenvolvimento aplicacional existente na IHM. Este exemplo contrapõe com alguma morosidade verificada nas medições a múltiplos sistemas e aplicações e até com a impossibilidade de medição noutros casos, por exemplo por não ter havido necessidade de reposição de dados ou de sistemas durante a fase de implementação.

Adicionalmente, restrições técnicas resultantes do processo iniciado na IHM para a renovação de equipamentos de rede, a substituição de cablagem para melhor suporte aos serviços e a desmaterialização de sistemas condicionaram a realização de algumas medições, como foi o cálculo da percentagem de acessos indevidos a VLANs (secção A.13.1.3).

Não obstante estas situações, os resultados obtidos e apresentados no Anexo XIII são muito importantes e permitem compreender quais as secções que requerem melhorias imediatas, na medida em que à maioria dos controlos foi possível aplicar uma fórmula/pontuação com código de cores elucidativo do nível de alerta.

Sobre a secção A.5, à data da entrega deste trabalho, o conjunto de políticas de segurança da informação proposto ao Conselho de Administração da IHM para aprovação da implementação encontra-se a aguardar a decisão deste órgão, tendo sido já aprovado pelas Chefias intermédias, nomeadamente o Chefe de Serviço e o Diretor de Serviços, ambos com responsabilidade pela área informática. A revisão das políticas, caso venham a ser aprovadas pelo CA, deve ocorrer anualmente ou após alterações significativas, o que justifica a ausência desse controlo de revisão nesta fase.

Os resultados da secção A.12, sobre a segurança de operações, revelam a necessidade de várias melhorias. O nível do desenvolvimento aplicacional com controlo de alterações (A.12.1.2) revela uma percentagem nula, sendo este um problema de segurança caso haja

necessidade de recurso a versões anteriores em resultado da deteção de falhas no desenvolvimento. Também a percentagem de ambientes separados (A.12.1.4), nomeadamente os ambientes de desenvolvimento, de teste e de produção, é baixa, sendo insegura a realização de operações nestas condições. A criação de ambientes distintos é fundamental para que apenas entrem em produção as aplicações validadas em ambiente de teste.

Já a gestão da capacidade em disco (A.12.1.3) revela a necessidade de acautelar o aumento da capacidade em 4 sistemas, seja através da instalação de capacidade adicional ou de migração para outro tipo de solução, pois permitir que um sistema atinja a máxima capacidade pode originar problemas graves de segurança para a informação nele contida. A existência deste controlo é importante para desencadear atempadamente os procedimentos necessários a garantir que a capacidade ocupada se mantém abaixo dos 60%.

Outras medições nesta secção indicam valores positivos, nomeadamente os controlos sobre *logs* de auditoria revistos, a sincronização de relógios com uma única referência horária, o software licenciado, a avaliação de vulnerabilidades em sistemas críticos desde a última grande *release* e a impossibilidade de instalação de software por parte dos utilizadores. Não obstante estes resultados indicarem bons níveis de segurança, novas medições devem ocorrer de acordo com a periodicidade definida. Por motivos distintos, alguns controlos não puderam ser aplicados tendo-se indicado essas justificações no Anexo XIII.

A secção A.13, sobre a segurança de comunicações, indica a necessidade de revisão dos dispositivos Bluetooth e dos protocolos para transferência segura de informação. Os restantes controlos de rede apresentam valores aceitáveis, no entanto os classificados com a cor "laranja" devem ser melhorados e monitorizados até à próxima medição para se aferir essa melhoria. A não medição de alguns controlos nesta secção deve-se a restrições decorrentes de atividades técnicas em curso na infraestrutura da empresa.

A gestão de incidentes de segurança da informação (secção A.16) indica a necessidade de melhorias. Os planos de resposta e de recuperação não se encontram concluídos, decorrendo daí um conjunto de dificuldades que afetariam a empresa em caso de ocorrência de incidentes, nomeadamente a não atribuição de papéis concretos para a execução de funções no âmbito da segurança e a indefinição na ordem de intervenção destes sobre um incidente. De referir que há um conjunto de funções e responsabilidades, normalmente definidas para este contexto, que se apresenta no Anexo V, e que não existem na empresa. Adicionalmente, a falta de técnicos e de estrutura não permite à equipa informática atual um melhor desempenho nos procedimentos de gestão de incidentes.

Na globalidade, é possível afirmar que a obtenção de resultados decorreu de forma satisfatória, no entanto, é notória a necessidade de intervenção a diversos níveis, nomeadamente sobre os controlos que requerem melhorias. Para complementar esta apreciação, os controlos são agora alvo de avaliação com recurso ao modelo de capacidade de processos da *framework* COBIT 5 [49, p. 44] e da escala de classificação da norma ISO/IEC

15504[7] [49, p. 48], ambos abordados no estado da arte, para que se possa obter uma imagem do estado de maturidade dos processos.

Tabela 16 - Modelo de capacidade de processos do COBIT 5 aplicado aos controlos implementados (exemplo)

Controlo	Nível	Capacidade do Processo	Escala
A.5.1.1 – Políticas para a segurança da informação	0	Incompleto	P - Parcialmente atingido
A.12.3.1 – Salvaguarda de informação	1	Executado	L – Amplamente atingido
A.13.1.1 – Controlos da rede (2 de 6)	0	Não implementado	N – Não atingido
A.16.1.2 – Reportar eventos de segurança da informação	0	Não implementado	N – Não atingido

A Tabela 16 apresenta um extrato da avaliação de capacidade realizada. O nível de capacidade obtido e a respetiva descrição da capacidade pode variar entre: 0 – Incompleto/Não implementado, 1 – Executado, 2 – Gerido, 3 – Estabelecido, 4 – Previsível e 5 – Otimizado.

A escala atingida em cada nível pode se situar entre: N - Não atingido, P - Parcialmente atingido, L - Amplamente atingido e F - Plenamente atingido.

Com a aplicação deste modelo de capacidade de processo é possível identificar não apenas os controlos que requerem maior atenção, mas mesmo dentro daqueles que se encontram no mesmo nível, compreender o patamar atingido em termos de escala. Toda esta informação ajuda na tomada de decisão sobre as melhorias a efetuar.

[7] A norma ISO/IEC 15504:2003, revista pela ISO/IEC 33002:2015, define os requisitos para a realização da avaliação de processo para utilização na melhoria dos processos e determinação da capacidade.

6. CONCLUSÕES E TRABALHO FUTURO

Seja a natureza do organismo pública ou privada, a informação produzida e em circulação, partilhada com outros organismos ou armazenada digitalmente, assim como o meio para a sua comunicação, são hoje ativos de grande valor fundamentais para o seu funcionamento. A proteção contra ameaças cada vez mais sofisticadas e destrutivas exige a adoção de medidas de gestão de riscos que permitam a máxima redução da possibilidade de ocorrências nos ativos da organização, tornando, assim, imperativa a implementação de mecanismos para a sua segurança.

Para dar resposta ao problema da ausência de políticas de segurança da informação identificado na empresa Investimentos Habitacionais da Madeira (IHM), conjugado com a necessidade de melhoria de processos neste contexto, iniciou-se o trabalho para alcançar o primeiro objetivo proposto, que consistiu na caraterização da IHM em termos de segurança. No seguimento, propôs-se uma metodologia que pretendeu tirar partido de normas existentes para a segurança da informação e das melhores práticas já testadas e implementadas em contexto empresarial, nomeadamente a norma NP ISO/IEC 27001:2013 e outras da mesma família, para executar um conjunto de processos no sentido de "estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação" (SGSI) [18, p. 6].

Com a metodologia definida alcançou-se o segundo objetivo estabelecido para este trabalho. O diagrama estabelecido coadunou-se com o ciclo PDCA – *Plan*, *Do*, *Check*, *Act* –, tendo sido possível, através de um conjunto de processos, efetuar um levantamento dos ativos de informação da empresa e obter o conhecimento dos riscos a estes associados. A gestão do risco, assente em processos de identificação, análise e avaliação permitiu preparar o tratamento a dar, especificar a Declaração de Aplicabilidade e desenvolver o programa de implementação do SGSI.

Sendo a norma NP ISO/IEC 27001:2013 abrangente a múltiplos domínios da segurança da informação, por motivos de restrição de tempo para a realização deste projeto optou-se por selecionar as 4 secções da norma cujos controlos se considerou serem mais prementes para a resolução do problema identificado. Em concreto, a secção A.5 - *Políticas de segurança de informação*, a secção A.12 - *Segurança de operações*, a secção A.13 - *Segurança de comunicações* e a secção A.16 - *Gestão de incidentes de segurança da informação*. Em particular, para melhor responder aos requisitos da secção A.16, recorreu-se à norma NIST SP 800-61r2, integrando-a com a norma NP ISO/IEC 27001:2013.

Ao longo do trabalho foram produzidos diversos artefactos operacionais, tais como políticas de segurança da informação, indicadores de desempenho para a medição de controlos, registos, procedimentos, entre outros. Especificou-se um conjunto de controlos para as secções escolhidas, tendo-se procedido à implementação da maioria destes e à sua medição ao longo de 30 dias com a finalidade de aferir as propostas de melhoria, alcançando, assim, o terceiro objetivo do trabalho.

Apesar de não ter sido possível definir controlos para todas as secções da norma NP ISO/IEC 27001:2013, da análise crítica aos resultados apresentados considera-se que a metodologia utilizada foi ajustada e os controlos definidos foram importantes para se obter uma visão inequívoca das necessidades de melhoria mais prementes, tendo para isto contribuído a utilização de um esquema cromático em conjunto com os critérios de pontuação dos controlos.

Sobre os novos controlos, não foi possível à data de entrega deste trabalho aferir o aumento do nível de segurança decorrente da aplicação de controlos que até então eram inexistentes, como é o caso das políticas de segurança, pelo facto de estas terem estarem a aguardar aprovação do Conselho de Administração da empresa.

Quanto aos controlos existentes, obteve-se como benefício um melhor conhecimento sobre quais as medidas de segurança que devem ser agilizadas, como por exemplo não permitir que o nível de ocupação da capacidade em disco ultrapasse os 60%, situação que se constatou em alguns equipamentos e que requereu ação imediata. Este exemplo demonstra como, com este controlo, foi possível tomar medidas para prevenir um problema que, caso contrário, poderia não ter sido detetado atempadamente, com consequências nos respetivos sistemas.

A aplicação posterior do Modelo de Capacidade de Processos do COBIT 5 foi também importante para se constatar que, apesar da importância da aplicação dos controlos, muitos continuam incompletos. Contribui para este facto a impossibilidade de, ao longo deste trabalho, se conseguir garantir a aplicação de todos os aspetos recomendados pela norma, como por exemplo o registo documental de todas as tarefas.

De referir que este trabalho decorreu em paralelo com algumas alterações significativas na infraestrutura informática da empresa e, por esse motivo, deverão ser desencadeadas novas medições dos controlos. Esta situação vem, no entanto, confirmar a versatilidade da metodologia proposta e a possibilidade de ser aplicada a cenários que envolvem mudanças. Tenha a empresa uma infraestrutura informática estabilizada ou esteja esta em atualização, a principal norma escolhida, NP ISO/IEC 27001:2013, é suportada pelo ciclo PDCA cuja génese é exatamente proporcionar melhorias ciclicamente.

Foram igualmente encontradas algumas dificuldades ao longo da execução deste trabalho, nomeadamente a impossibilidade de consulta das normas ISO através da entidade governamental responsável pela área da Qualidade. Foi, também, fator condicionante a existência de poucas fontes internas à empresa que dispusessem de conhecimentos suficientemente profundos sobre processos associados à informação. Este obstáculo foi, no entanto, ultrapassado com recurso à experiência empregue nas tarefas realizadas diariamente.

Como aspeto positivo, pelos resultados obtidos crê-se que a melhoria da segurança através da aplicação de políticas e adequação dos processos a uma melhor proteção da informação venha a ter consequências positivas no serviço informático, inclusivamente nos planos de investimento para os anos vindouros e nos gastos não previstos, pois a prevenção de situações

de risco e a monitorização de eventos de segurança pode evitar despesas de avultado montante, normalmente inevitáveis em situação de incidente grave.

Em resumo, considera-se que o problema identificado foi parcialmente resolvido com a aplicação da metodologia proposta, nomeadamente através da definição de políticas e da aplicação de controlos, cuja medição permitiu determinar o nível de segurança e iniciar a respetiva melhoria no decurso das atividades informáticas. A resolução completa do problema está condicionada por vários fatores, nomeadamente no planeamento das atividades informáticas e das tarefas específicas a realizar, que deverão ter sempre presente os requisitos de segurança, a redefinição de alguns métodos de trabalho técnico que permitam passar do conhecimento tácito ao cumprimento de procedimentos especificados, o registo documental por regra e o maior envolvimento de todos os colaboradores da empresa em ações de consciencialização para a segurança da informação.

Em termos de certificação, como definido no objetivo e campo de aplicação da norma NP ISO/IEC 27001:2013, "a exclusão de quaisquer dos requisitos especificados nas secções 4 a 10 não é aceitável para uma organização que reivindica a sua conformidade face a esta Norma" [18]. Assim, não pode nesta fase a IHM almejar a obtenção de conformidade com a referida norma por não estar completo todo o processo que permite "estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação" (SGSI) [18, p. 6].

Para esse objetivo, propõe-se que trabalho futuro relacionado com este projeto passe pelo cumprimento integral dos requisitos especificados da norma NP ISO/IEC 27001:2013, condição sine qua non para iniciar o processo de obtenção da certificação que, crê-se, elevará o nome da IHM ao patamar das empresas referência no que à conformidade com as melhores práticas diz respeito.

Adicionalmente, sugere-se a implementação de uma solução open *source* para a gestão da segurança da informação, nomeadamente para suporte e melhoria na execução de diversos processos, tais como o registo de ativos e a gestão do risco. Um exemplo é a aplicação verinice[8], que permite estabelecer, manter e melhorar um SGSI baseado em diversas normas e ainda dispõe de funcionalidades de auditoria, gestão de documentos, produção de relatórios, entre outras. Esta aplicação é disponibilizada para *Windows*, *Linux* e *MacOS* [69].

[8] Verinice - https://verinice.com/en/

GLOSSÁRIO

Access Point (AP). Dispositivo de hardware ou um nó configurado numa rede local (LAN) que permite a conexão entre dispositivos sem fios e redes com fios através de um protocolo (e.g. Wi-Fi ou Bluetooth). Os APs possuem transmissores e antenas de rádio que facilitam a conectividade.

Adaptador Ethernet. *Hardware* que permite que um dispositivo ou posto de trabalho aceda a uma conexão *Ethernet*.

Aplicação *client-side*. *Software* que é executado nos computadores que representam os clientes.

Aplicação forense. *Software* utilizado no processo de descoberta e interpretação de dados com o objetivo de preservar qualquer evidência na sua forma mais original enquanto é realizada uma investigação estruturada através da recolha, identificação e validação da informação digital com o propósito de reconstruir eventos passados.

Aplicação *Web*. Programa acedido através de uma ligação de rede, utilizando HTTP e, normalmente, executado num navegador *Web*. Este tipo de aplicação pode também ser baseado no cliente, onde uma pequena parte do programa é descarregada para a área de trabalho do utilizador, mas o processamento é efetuado pela Internet num servidor externo.

Ataque cibernético ou ciberataque. Um ciberataque é a exploração deliberada de sistemas informáticos de empresas e redes dependentes de tecnologia. Os ciberataques utilizam códigos maliciosos para alterar o código, a lógica ou os dados do computador, com consequências disruptivas que podem comprometer os dados e levar a crimes cibernéticos, como por exemplo a alteração de informações ou o roubo de identidade.

Ataque de negação de serviços (*Denial of Service* (DoS)). Ataque em que os *hackers* tentam impedir que utilizadores legítimos acedam a serviços ou recursos na rede. O atacante normalmente envia um elevado número de mensagens, solicitando que a rede ou o servidor autentiquem solicitações com endereços de retorno inválidos. A rede ou o servidor não conseguirá encontrar o endereço de retorno ao enviar a aprovação de autenticação, fazendo com que o servidor espere antes de terminar a ligação. Quando o servidor termina a ligação, o atacante envia mais mensagens, havendo uma repetição do processo que acaba mantendo a rede ou o servidor ocupado.

Ataque por força bruta. Um ataque de força bruta é um método de tentativa e erro utilizado para obter informações, como uma palavra-passe de utilizador ou um número de identificação pessoal (PIN). Num ataque de força bruta é utilizado *software* para gerar um grande número de tentativas consecutivas quanto ao valor dos dados desejados. Os ataques de força bruta

podem ser utilizados por *hackers* para decifrar informação encriptada, ou por analistas de segurança para testar a segurança de rede de uma organização.

Ataque *Web-based*. Ataques com foco na aplicação e nas funções da camada 7 do modelo OSI.

***Backup*.** Processo de efetuar cópias de segurança de dados para utilizar caso os dados originais sejam perdidos ou destruídos.

***Backup* Completo.** Contém todos os dados.

***Backup* Incremental.** Contém apenas os dados que foram alterados desde a execução de um *backup* anterior. O *backup* anterior pode ser um *backup* completo ou um *backup* incremental adicional.

***Backup* Diferencial.** Contém apenas as alterações ocorridas desde o *backup* completo mais recente.

***Bad block*.** Parte ou subdivisão inutilizável de uma faixa no disco rígido. Normalmente resulta de danos físicos. Uma vez que o bloco (ou sector) defeituoso é identificado pelo *software* utilitário de disco (e.g. CHKDSK em sistemas Microsoft), este programa marca os setores com falha para que o sistema operativo possa ignorá-los no futuro.

***Bluetooth*.** *Standard* aberto de tecnologia sem fios para a transmissão de dados de dispositivos eletrónicos fixos e móveis a curtas distâncias. O *Bluetooth* permite a comunicação com uma variedade de dispositivos (e.g. players MP3/MP4, periféricos e computadores pessoais).

***Botnet*.** Grupo de computadores conectados de forma coordenada para fins maliciosos. Cada computador numa *botnet* é denominado *bot*. Os *bots* formam uma rede de computadores comprometidos, que é controlada por terceiros e utilizada para transmitir *malware* ou *spam*, ou para lançar ataques.

***Bring Your Own Device* (BYOD).** Refere-se a funcionários que trazem para a empresa os seus próprios equipamentos/dispositivos de computação (e.g. *smartphones*, *laptops* e *tablets*) para utilizá-los conjuntamente ou em vez dos equipamentos fornecidos pela empresa. Também pode ser referido como "traga a sua própria tecnologia" (BYOT).

***Computer Emergency Response Team* (CERT).** Equipa especializada e treinada para monitorizar, identificar e responder a incidentes de segurança. Lida com a evolução de *malware*, vírus e outros ciberataques.

Certificação de sistema. Processo de avaliação técnica abrangente dos componentes de um sistema e da sua conformidade.

Certificação profissional. Processo de validação das capacidades e conhecimentos adquiridos e comprovados por especialistas.

***Chat*.** Processo de comunicação, interação e/ou troca de mensagens pela Internet. Envolve dois ou mais indivíduos que se comunicam através de um serviço ou *software* desenvolvido para conversação.

Ciberespaço. Espaço ou conjunto das comunidades de redes de comunicação entre computadores, nomeadamente a Internet.

Cibersegurança. Métodos preventivos utilizados para proteger o ataque, o comprometimento ou o roubo de informação, que requerem um entendimento das possíveis ameaças (e.g. vírus e outros códigos maliciosos). Estratégias de cibersegurança incluem a gestão de identidades, a gestão de riscos e a gestão de incidentes.

Cliente-servidor. Modelo de computação no qual o servidor armazena, entrega e gere a maioria dos recursos e serviços a serem consumidos pelo cliente. Nesta arquitetura, um ou mais computadores (clientes) estão ligados a um servidor através de uma conexão de rede ou de internet.

***Demilitarized Zone* (DMZ).** *Host* ou rede que atua como caminho intermediário e seguro entre a rede interna de uma organização e a rede externa ou não-proprietária. Uma DMZ é a linha da frente que interage diretamente com as redes externas, ao mesmo tempo que as separa logicamente da rede interna. Também é conhecida como perímetro da rede.

***Domain Name System Security Extensions* (DNSSEC).** Conjunto de extensões de segurança que fornece aos clientes DNS a autenticação de origem de todos os dados DNS e integridade. Não fornece confidencialidade ou disponibilidade.

***Dual-factor*.** Mecanismo de segurança que requer dois tipos de credenciais para autenticação. Ao ter sido projetado para fornecer uma camada adicional de validação, minimiza as violações de segurança.

***End-point*.** Dispositivo que atua na extremidade de um sistema distribuído. Normalmente, refere um PC conectado à Internet numa rede TCP/IP.

***Enterprise Resource Planning* (ERP).** Conjunto de aplicações de *software* ou um único pacote (mas mais complexo) que disponibiliza os dados exigidos por duas ou mais áreas de negócio da organização.

Envelope. Mecanismo utilizado para proteger uma mensagem eletrónica através de encriptação e autenticação.

Firewall. *Software* utilizado para manter a segurança de uma rede privada. Bloqueia o acesso não autorizado de ou para redes privadas e pode ser implementada utilizando *hardware*, *software* ou uma combinação de ambos.

Firmware. *Software* gravado permanentemente num dispositivo de *hardware* e que está programado para fornecer instruções de comunicação com outros dispositivos e executar funções, como por exemplo tarefas básicas de entrada/saída. O *firmware* é normalmente armazenado na memória ROM e pode ser atualizado.

***File Transfer Protocol* (FTP).** Protocolo cliente/servidor utilizado para transferência de ficheiros, que pode ser autenticado com nome de utilizador e palavra-passe. O FTP anónimo permite que o utilizador aceda a ficheiros, programas e outros dados da Internet sem a necessidade de um ID ou palavra-passe.

Hash. Função matemática que recebe um grupo de caracteres e mapeia-os para um valor de um determinado comprimento chamado de *hash value* ou *hash*. O *hash* é muitas vezes utilizado para indexar e localizar itens em bases de dados, pois é mais fácil encontrar o valor de *hash* (mais curto) do que a cadeia mais longa. O *hashing* também é utilizado na criptografia.

Helpdesk. Departamento ou serviço numa organização que é responsável por dar resposta às questões técnicas dos utilizadores.

Home banking. Serviços bancários em que os clientes de um banco podem gerir as suas contas pela Internet em vez de visitar uma agência ou utilizar o telefone. O banco *online* é normalmente composto por uma ligação de dados segura.

Hot-swap. Capacidade de substituir ou instalar um componente sem desligar o computador. O *hot-swap* permite um fácil acesso à componente a substituir e a conveniência de sistemas ininterruptos.

***Hypertext Transfer Protocol Secure* (HTTPS).** Variante do protocolo de transferência da *Web* (HTTP) padrão que adiciona uma camada de segurança aos dados em circulação através de SSL (*Secure Socket Layer*) ou protocolo TLS (*Transport Layer Security*). O HTTPS permite comunicação encriptada e ligação segura entre um utilizador remoto e o servidor *Web*.

Indicador. Sinal de que um incidente já ocorreu ou poderá estar a ocorrer no momento.

***Intrusion Detection System* (IDS).** *Software* de segurança projetado para alertar automaticamente os administradores quando alguém ou algo está tentando comprometer o sistema de informações através de atividades mal-intencionadas ou de violações da política de segurança. Um IDS monitoriza a atividade do sistema examinando as vulnerabilidades, a integridade dos ficheiros e realizando uma análise de padrões com base em ataques já conhecidos.

***Intrusion Prevention System* (IPS).** Sistema que monitoriza uma rede à procura de atividades maliciosas como sejam ameaças de segurança ou violações de políticas. A principal função de um IPS é identificar atividades suspeitas, registrar essas informações, tentar bloquear as atividades e, finalmente, reportá-las.

***Intrusion Detection and Prevention System* (IDPS).** Sistema conjunto de deteção (IDS) e prevenção (IPS) de intrusões.

***Integrated Lights-Out* (iLO).** Consola *Web* que pode ser utilizada para administrar um servidor remotamente. A placa de gestão do iLO tem a sua própria conexão de rede e endereço IP ao qual os administradores do servidor se podem conectar via DNS (*Domain Name System*)/DHCP.

Imagem do sistema. Ficheiro único ou dispositivo de armazenamento que contém uma réplica de todos os dados de um sistema. Geralmente, uma imagem de disco é criada através de uma replicação setor-a-setor do armazenamento original - ou de origem, incluindo a estrutura (diretórios e pastas) e o conteúdo (ficheiros).

***Internet of Things* (IoT).** Conceito de computação que descreve a ideia de objetos físicos do dia-a-dia conectados à Internet e capazes de se identificar com outros dispositivos. O termo está associado ao RFID (*Radio-Frequency Identification*) como tecnologia de comunicação, embora também possa incluir outras tecnologias de sensores, tecnologias sem fio ou códigos QR.

***Internet Protocol* (IP).** Endereço numérico lógico atribuído a cada computador, impressora, *switch*, *router* ou qualquer outro dispositivo que faça parte de uma rede baseada em TCP/IP. O endereço IP é o componente principal a partir do qual a arquitetura de rede é construída. Os endereços IP são divididos em duas partes: a parte da rede, que especifica a que rede este endereço pertence; a parte do *host*, que indica o equipamento exato.

***Internet Protocol Security* (IPSec).** Conjunto de protocolos que fornece segurança para o protocolo da Internet. Pode ser usado para a configuração de redes privadas virtuais (VPNs) de maneira segura.

O IPSec envolve dois serviços de segurança: o *Authentication Header* (AH), que autentica o remetente e deteta quaisquer alterações nos dados durante a transmissão; o *Encapsulating Security Payload* (ESP), que não apenas realiza a autenticação do remetente, mas também encripta os dados que estão sendo enviados.

Existem dois modos de IPSec: o *Modo de Túnel*, que leva todo o pacote IP para formar uma comunicação segura entre dois locais ou *gateways*; o *Modo de Transporte*, que encapsula somente o *payload* (carga útil) do IP e não o pacote IP inteiro como no modo de encapsulamento (modo de túnel) para garantir um canal seguro de comunicação.

***Knowledge base*.** Base de dados utilizada para partilha e gestão de conhecimento. Promove a recolha, organização e recuperação de conhecimento. Muitas bases de conhecimento são estruturadas com recurso a técnicas de inteligência artificial e não apenas armazenamento de dados, para encontrarem soluções para problemas futuros utilizando dados de experiências anteriores armazenadas como parte da base de conhecimento. Os sistemas de gestão de conhecimento dependem de tecnologias de gestão de dados que vão desde bases de dados relacionais a data *warehouses*.

***Local Area Network* (LAN).** Rede de computadores numa área geográfica pequena, composta por computadores pessoais capazes de aceder a dados e dispositivos como impressoras, *scanners* e dispositivos de armazenamento em qualquer lugar da LAN. As LANs são caracterizadas por taxas de comunicação e transferência de dados elevadas.

***Link* (estático).** Código que contém um URL permanente ou imutável. É o oposto do *link* dinâmico. Sendo permanente por natureza, os motores de busca consideram estes links mais fáceis de rastrear e indexar, o que ajuda na otimização de mecanismos de busca (SEO).

***Log*.** Recurso que ajuda a fornecer informações sobre tráfego de rede, utilização e outras condições. Um *log* de eventos armazena dados para recuperação por profissionais de segurança ou sistemas de segurança automatizados para ajudar os administradores de rede a gerir aspetos como a segurança, o desempenho e a transparência.

***Media Access Control Address* (MAC Address).** Identificador exclusivo para uma Ethernet ou um adaptador de rede numa rede de dados. Um endereço MAC também é conhecido como endereço físico ou endereço de *hardware*.

***Malware*.** Qualquer *software* que cause danos a um sistema informático. Pode ser na forma de worm, vírus, trojan, spyware, adware, rootkit, etc. e tem a capacidade de roubar dados protegidos, eliminar documentos ou adicionar *software* não aprovado pelo utilizador.

***Network Attached Storage* (NAS).** Servidor dedicado, também chamado de *appliance*, utilizado para armazenamento e partilha de ficheiros, mas que não permite outros serviços como *e-mails* ou autenticação.

***Network Time Protocol* (NTP).** Permite a sincronização de relógios de computador distribuídos pela rede, garantindo a precisão da hora local com referência a algum momento específico da Internet. O NTP comunica entre clientes e servidores utilizando o *User Datagram Protocol* (UDP) na porta 123.

***Organizationally Unique Identifier* (OUI).** Número de 24 bits que identifica exclusivamente um fornecedor ou fabricante.

***Patch*.** Atualização de *software* composta por código adicionado ou corrigido num programa executável. Normalmente, um *patch* é instalado sobre um programa de software existente. Os *patches* são, geralmente, correções temporárias entre versões completas de um pacote de *software*.

PDCA – *Plan, Do, Check, Act*. Ciclo de quatro etapas para a resolução de problemas e melhoria contínua que inclui o planeamento, a implementação, a verificação dos resultados e a ação.

***Phishing*.** Ato fraudulento de adquirir informações privadas e confidenciais tais como números de cartão de crédito, identificação pessoal e contas de utilizador e palavras-passe. Utilizando um conjunto complexo de técnicas de engenharia social e experiência em programação, os *sites* de *phishing* atraem os destinatários de *e-mail* e os utilizadores da *Web* levando-os a acreditar que o *site* falso é legítimo e genuíno. Mais tarde a vítima descobre que a sua identidade pessoal e outras informações vitais foram roubadas e expostas.

***Port isolation*.** Garantia que uma porta num *switch* apenas comunica com o *uplink*, não podendo comunicar com outros recursos na mesma sub-rede.

Precursor. Sinal de que um incidente pode ocorrer no futuro.

Ransomware. Tipo de *malware* que infecta, bloqueia ou assume o controlo de um sistema e exige um resgate para repor a normalidade. O *ransomware* ataca e infecta um computador com a intenção de extorquir dinheiro.

Realidade aumentada. Ambiente de exibição interativo, baseado na realidade, que aproveita as capacidades de visualização, som, texto e efeitos gerados por computador para melhorar a experiência do utilizador. A realidade aumentada combina cenas e imagens reais e baseadas em computador para oferecer uma visão unificada, mas aperfeiçoada do mundo.

Recuperação "bare metal". Processo de restauro do sistema no qual uma imagem/instância de computador idêntica é criada num computador a partir do zero. Permite que um computador seja restaurado sem *software* pré-instalado, à exceção do *firmware* ou da BIOS. A restauração *bare-metal* também é conhecida como restauração de camada 1 (tier 1).

***Redundant Array of Inexpensive Disks* (RAID).** Método de armazenamento de dados em dois ou mais discos rígidos para fins de *backup*, tolerância a falhas, melhoraria da taxa de transferência, aumento da capacidade de armazenamento e melhoria do desempenho. O RAID é obtido combinando dois ou mais discos rígidos e um controlador RAID numa unidade lógica. O sistema operativo vê o RAID como um único disco rígido lógico chamado *array*. Existem diferentes níveis de RAID, em que cada um distribui os dados pelos discos rígidos com seus próprios atributos e características.

Regulamento da União Europeia. Ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países.

Regulamento administrativo. Norma jurídica geral e abstrata que no exercício de poderes jurídico-administrativos visa produzir efeitos jurídicos externos. É um normativo de grau inferior ao ocupado pela lei, que visa pormenorizá-la e complementá-la com o intuito de viabilizar a sua aplicação ou execução.

***Release*.** Processo de lançamento de um novo produto para um mercado específico ou base de utilizadores. No desenvolvimento de *software*, uma versão do produto é, por vezes, lançada numa versão beta para que programadores e utilizadores possam ajudar com a depuração e com *feedback* antes do lançamento do *software* final.

***Remote Desktop*.** Software proprietário da Microsoft para assistência remota.

Roubo de dados. Transferência ou armazenamento ilegal de qualquer informação de natureza confidencial, pessoal ou financeira, incluindo palavras-passe, código de software ou algoritmos, informações proprietárias orientadas a processos ou tecnologias. É uma violação de segurança e de privacidade com consequências graves para indivíduos e empresas.

Router. Dispositivo que analisa o conteúdo dos pacotes de dados transmitidos numa rede ou para outra rede. Os *routers* determinam se a origem e o destino estão na mesma rede ou se os dados devem ser transferidos de um tipo de rede para outro, o que requer o encapsulamento do pacote de dados com informações de cabeçalho do protocolo de encaminhamento (*routing*) para o novo tipo de rede.

***Script*.** Lista de comandos executados por determinados programas. Geralmente são documentos de texto com instruções escritas, utilizados para gerar páginas *Web* e para automatizar processos.

***Secure Shell* (SSH).** Protocolo criptográfico para a execução de serviços de rede, serviços de *shell* e comunicação de rede segura com um computador remoto. Permite que dois utilizadores conectados remotamente efetuem a comunicação de rede e utilizem serviços sobre uma rede não segura (e.g. internet).

***Service Level Agreement* (SLA).** Contrato entre o cliente e o fabricante e/ou prestador de serviços que estabelece os termos dos serviços a prestar (e.g. condições que permitam minimizar os tempos de recuperação dos sistemas e aplicações).

***Service Set Identifier* (SSID).** Identificador exclusivo de uma rede local sem fios (WLAN). Permite diferenciar as LANs sem fio atribuindo um identificador de caractere alfanumérico de 32 bits exclusivo a cada WLAN. Também é conhecido como um nome de rede.

Servidor. Computador, dispositivo ou programa dedicado à gestão de recursos de rede. É um equipamento normalmente dedicado porque quase não realiza outras tarefas para além das tarefas de servidor. Existem várias categorias de servidores, incluindo servidores de impressão, servidores de ficheiros, servidores de rede e servidores de bases de dados.

***Slack*.** Ocorre quando existe fragmentação interna no disco rígido, isto é, quando os ficheiros são armazenados em *clusters* (áreas de armazenamento com alocação muito pequena) cada ficheiro é gravado automaticamente no início de um *cluster*, criando uma potencial lacuna (*slack*) entre os *bytes* do primeiro ficheiro e os *bytes* do último ficheiro.

***Sniffer*.** Ferramenta que intercepta dados que circulam numa rede. A placa de rede é colocada em modo promíscuo e lê as comunicações entre computadores dentro de um segmento específico, permitindo que o *sniffer* obtenha toda a informação que está em circulação na rede, podendo originar o acesso não autorizado a dados confidenciais. Também é conhecido como analisador de pacotes.

***Software as a Service* (SaaS).** Modelo de distribuição de *software* onde os clientes acedem ao *software* pela Internet. As principais características são as atualizações aplicadas automaticamente sem intervenção do cliente, o serviço ser adquirido por assinatura e não ser necessário instalar nenhum *hardware* por parte do cliente.

***Spam*.** Utilização de sistemas de mensagens eletrónicas para o envio massivo de mensagens não solicitadas ou indesejadas.

***Secure Socket Layer/Transport Layer Security* (SSL/TLS).** O SSL é um protocolo padrão utilizado para uma transmissão segura numa rede, em que é criado um *link* seguro entre um servidor *Web* e um navegador para garantir a transmissão de dados privada e integral. O SSL usa o protocolo TCP para comunicação. O TLS é um protocolo que fornece segurança de comunicação a nível de privacidade, integridade e proteção dos dados transmitidos entre diferentes nós na Internet. O TLS é um sucessor do protocolo SSL.

Switch. Dispositivo de alta velocidade que recebe pacotes de dados e os redireciona para o seu destino numa rede local (LAN). Um *switch* LAN opera na camada de ligação ou na camada de rede do Modelo OSI e, como tal, pode suportar todos os tipos de protocolos de pacotes.

Symmetric Stream Cypher. Cifra em que dígitos em texto livre são combinados com um fluxo de dígitos encriptados aleatoriamente (fluxo de chaves). Cada dígito de texto livre é encriptado (um de cada vez) com o dígito correspondente do fluxo de chaves, para produzir um dígito do fluxo de texto cifrado.

***Tape*.** Dispositivo de armazenamento baseado em fita magnética, utilizado para armazenar diferentes tipos de dados digitais.

***Teamviewer*.** *Software* proprietário para assistência remota.

***Telnet*.** Protocolo de rede e programa de *software* utilizado para o acesso a computadores e terminais remotos através da Internet ou de uma rede TCP/IP. O Telnet envia todas as mensagens em texto livre e não possui mecanismos de segurança específicos. A sua utilização não é recomendada.

Timestamp. Informação temporal referente a um evento registado pelo computador e armazenado como um *log* ou como meta-dados. Qualquer evento ou atividade pode ter um registo de data e hora, dependendo das necessidades do utilizador ou dos recursos do processo que cria o registo de data e hora.

***Uplink*.** Ligação para envio de dados para o núcleo da rede.

Vetor de ataque. Técnica utilizada por *hackers* para fins nocivos, através da qual o acesso não autorizado pode ser obtido para um dispositivo ou uma rede. Os vetores de ataque ajudam indivíduos não autorizados a explorar as vulnerabilidades no sistema ou na rede, incluindo os elementos humanos.

Virtualização. Criação de recursos virtuais, de forma escalável, que permite tirar melhor aproveitamento do *hardware* através de processos de emulação.

VNC. Software *open-source* para assistência remota.

VPN. Rede privada construída sobre uma infraestrutura pública. Mecanismos de segurança como a criptografia permitem que os utilizadores acedam com segurança a uma rede a partir de diferentes locais através de uma rede pública, frequentemente a Internet.

***Wi-Fi* 802.11.** Conjunto de normas que definem a comunicação para LANs sem fios (WLANs).

***Windows Time service* (W32Time).** Serviço Microsoft que sincroniza a data e a hora de todos os computadores em execução no AD DS (Serviços de Domínio Active Directory). O W32Time utiliza o protocolo NTP (*Network Time Protocol*) para sincronizar os relógios do computador na rede.

WPA2 802.11i - *Robust Security Network*. Protocolo de rede para proteção de computadores ligados a uma rede Wi-Fi, tem como objetivos a conformidade total com o padrão IEEE802.11i, que era apenas parcialmente atingida com o WPA.

***Zero-day*.** Tipo de falha de *software* ou falha de segurança desconhecida ou imprevista num sistema que pode ser explorada por *hackers*.

REFERÊNCIAS

[1] C. Timberg, *The Threatened Net: How the Web Became a Perilous Place*, The Washington Post. New York, NY: Diversion Books, 2015.

[2] European Union Agency for Network and Information Security (ENISA), *ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends*, 1.0. Heraklion: European Union Agency for Network and Information Security Publishing, 2018.

[3] ISACA, «State of Cybersecurity 2018: Threat Landscape and Defense Techniques». ISACA, Jun-2018.

[4] Direção-Geral da Política de Justiça, «RASI - Relatório Anual de Segurança Interna 2017». Gabinete do Secretário-Geral, Mar-2018.

[5] L. Wang e R. Ranjan, «Processing Distributed Internet of Things Data in Clouds», *IEEE Cloud Comput.*, vol. 2, n. 1, pp. 76–80, Fev. 2015.

[6] M. A. Morsy, J. Grundy, e I. Müller, «An Analysis of the Cloud Computing Security Problem», *Swinburne Univ. Technol. Hawthorn Vic. Aust.*, p. 6, Jan. 2010.

[7] H. São Mamede, *Segurança Informática nas Organizações*, vol. 1, 1 vols. FCA - Editora de Informática, Lda., 2006.

[8] A. A. Forni e R. van der Meulen, «Gartner Says Detection and Response is Top Security Priority for Organizations in 2017», Mar-2017. [Em linha]. Disponível em: https://www.gartner.com/newsroom/id/3638017.

[9] União Europeia e Jornal Oficial da União Europeia, *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. 2016, pp. 1–88.

[10] European Committee for Standardization, «What is a Standard?», *What is a Standard?*, 2018. [Em linha]. Disponível em: https://www.cen.eu/work/ENdev/whatisEN/Pages/default.aspx.

[11] European Union Agency for Network and Information Security (ENISA), «Standards and certification — ENISA», *Standards and certification — ENISA*. [Em linha]. Disponível em: https://www.enisa.europa.eu/topics/standards.

[12] S. Harris e F. Maymí, *CISSP Exam Guide*, Seventh edition. New York: McGraw-Hill Education, 2016.

[13] E. Conrad, S. Misenar, e J. Feldman, *CISSP Study Guide*, Third edition., vol. 1, 1 vols. Amsterdam; Boston: Elsevier, 2016.

[14] Diário da República, *Decreto-Lei n.º 4/2015, Código do Procedimento Administrativo*. 2017, pp. 50–87.

[15] «Portal Europeu da Justiça», Jul-2017. [Em linha]. Disponível em: https://e-justice.europa.eu/content_member_state_law-6-pt-maximizeMS-pt.do?member=1.

[16] União Europeia, «Regulamentos, diretivas e outros atos legislativos», 16-Jun-2016. [Em linha]. Disponível em: https://europa.eu/european-union/eu-law/legal-acts_pt.

[17] União Europeia, «Regulamentos da União Europeia», *EUR-Lex - l14522*, Ago-2015. [Em linha]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14522.

[18] IPQ - Instituto Português da Qualidade, I.P., «NP ISO/IEC 27001:2013 - Tecnologia de informação -- Técnicas de segurança -- Sistemas de gestão de segurança da informação - Requisitos». IPQ - Instituto Português da Qualidade, I.P., 2013.

[19] ISO/IEC JTC 1/SC 27, «ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls». International Organization for Standardization, Out-2013.

[20] ISO/IEC JTC 1/SC 27, «ISO/IEC 27003:2010 - Information technology -- Security techniques -- Information security management system implementation guidance». International Organization for Standardization, Fev-2010.

[21] ISO/IEC JTC 1/SC 27, «ISO/IEC 27004:2016 - Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation». International Organization for Standardization, Dez-2016.

[22] ISO/IEC JTC 1/SC 27, «ISO/IEC 27005:2011 - Information technology -- Security techniques -- Information security risk management». International Organization for Standardization, Jun-2011.

[23] IPQ - Instituto Português da Qualidade, I.P., «NP ISO 31000:2012 -- Gestão do risco -- Princípios e linhas de orientação». IPQ - Instituto Português da Qualidade, I.P., Jul-2012.

[24] ISACA, «COBIT 5: A Business Framework for the Governance and Management of Enterprise IT», Abr-2012. [Em linha]. Disponível em: http://www.isaca.org/COBIT/pages/cobit-5.aspx.

[25] C. J. Alberts, S. G. Behrens, R. D. Pethia, e W. R. Wilson, «Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0», Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, Technical rept. 99-TR-017, Jun. 1999.

[26] M. P. Barret, «Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1», *Natl. Inst. Stand. Technol.*, Abr. 2018.

[27] (ISC)2 - International Information System Security Certification Consortium, «Certified Information Systems Security Professional», 2018. [Em linha]. Disponível em: https://www.isc2.org/Certifications/CISSP.

[28] (ISC)2 - International Information System Security Certification Consortium, «Certified Secure Software Lifecycle Professional», 2018. [Em linha]. Disponível em: https://www.isc2.org/Certifications/CSSLP.

[29] (ISC)2 - International Information System Security Certification Consortium, «Certified Cloud Security Professional», 2018. [Em linha]. Disponível em: https://www.isc2.org/Certifications/CCSP.

[30] (ISC)2 - International Information System Security Certification Consortium, «Certified Authorization Professional», 2018. [Em linha]. Disponível em: https://www.isc2.org/Certifications/CAP.

[31] ISACA, «Certified Information Systems Auditor (CISA)», 2018. [Em linha]. Disponível em: http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx.

[32] ISACA, «Certified Information Security Manager (CISM)», 2018. [Em linha]. Disponível em: http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx.

[33] ISACA, «Certified in Risk and Information Systems Control (CRISC)», *Certified in Risk and Information Systems Control - IT Certification - CRISC | ISACA*, 2018. [Em linha]. Disponível em: http://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Pages/default.aspx.

[34] CompTIA, «CompTIA Security+ Certification», *CompTIA Security+ Certification*, 2018. [Em linha]. Disponível em: https://certification.comptia.org/certifications/security.

[35] EC-Council, «Certified Network Defender Certification», 2018. [Em linha]. Disponível em: https://www.eccouncil.org/programs/certified-network-defender-cnd/.

[36] EC-Council, «Certified Ethical Hacker Certification», 2018. [Em linha]. Disponível em: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/.

[37] GIAC, «Security Certification: GSEC», 2018. [Em linha]. Disponível em: https://www.giac.org/certification/security-essentials-gsec.

[38] GIAC, «Security Certification: GISF», 2018. [Em linha]. Disponível em: https://www.giac.org/certification/information-security-fundamentals-gisf.

[39] GIAC, «Security Certification: GCED», 2018. [Em linha]. Disponível em: https://www.giac.org/certification/certified-enterprise-defender-gced.

[40] União Europeia, «Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho», *Jornal Oficial da União Europeia*, p. 30, 06-Jul-2016.

[41] H. Susanto, M. N. Almunawar, e Y. C. Tuan, «Information Security Management System Standards: A Comparative Study of the Big Five», *Int. J. Electr. Comput. Sci. IJECS-IJENS*, vol. 11, n. 05, p. 7, Out. 2011.

[42] International Organization for Standardization, «About ISO», 2018. [Em linha]. Disponível em: https://www.iso.org/about-us.html.

[43] International Organization for Standardization, «The ISO Survey», 2016. [Em linha]. Disponível em: https://www.iso.org/the-iso-survey.html?certificate=ISO%209001&countrycode=AF.

[44] R. V. Fazenda e L. L. Fagundes, «Analysis of the challenges faced in establishing and maintaining an information security management system on the Brazilian scene», XI Brazilian Symposium on Information Systems, Goiás, Brazil, 2015, vol. 1, p. 41.

[45] R. D. Moen e C. L. Norman, «Evolution of the PDCA cycle», Seventh Asian Network for Quality Congress, Tokyo, 2009.

[46] E. Humphreys, «Information security management standards: Compliance, governance and risk management», *Inf. Secur. Tech. Rep.*, vol. 13, n. 4, pp. 247–255, Nov. 2008.

[47] S. S. Greene, *Security Policies and Procedures: Principles and Practices*, 1.ª ed. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2005.

[48] R.E. Smith, Elementary Information Security, Second edition. Jones & Barlett Learning, 2015.

[49] ISACA, «COBIT 5: Modelo Corporativo para Governança e Gestão de TI da Organização». ISACA, 2012.

[50] ISACA, «CISA Certification Job Practice», 2016. [Em linha]. Disponível em: http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Job-Practice-Areas/Pages/CISA-Job-Practice-Areas.aspx#domain2.

[51] ISO/IEC JTC 1/SC 27, «ISO/IEC 27035-1:2016 - Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management», Nov-2016. [Em linha]. Disponível em: https://www.iso.org/standard/60803.html.

[52] ISO/IEC JTC 1/SC 27, «ISO/IEC 27035-2:2016 - Information technology -- Security techniques -- Information security incident management -- Part 2: Guidelines to plan and prepare for incident response», Nov-2016. [Em linha]. Disponível em: https://www.iso.org/standard/62071.html.

[53] ISECT Ltd., «ISO/IEC 27035 Information security incident management», Set-2011. [Em linha]. Disponível em: http://www.iso27001security.com/html/27035.html.

[54] ISACA, *COBIT Self-assessment Guide: Using COBIT 5*, 2.ª ed. Rolling Meadows, Illinois: ISACA, 2013.

[55] ISACA, «CISA Online Review Course», 2018. [Em linha]. Disponível em: http://www.isaca.org/Education/on-demand-learning/Pages/cisa-online-review-course.aspx.

[56] P. Cichonski, T. Millar, T. Grance, e K. Scarfone, «NIST Special Publication 800-61r2 Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology», National Institute of Standards and Technology, Gaithersburg, MD, Ago. 2012.

[57] H. Correia e APCER, «Ferramentas de gestão no sector das Tecnologias de Informação - Apresentação realizada no evento "Inovação e robustez da engenharia dos sistemas de informação para potenciar o reconhecimento internacional", Strongstep - FEUP - Porto», Porto, Nov-2010.

[58] IHM, EPERAM, «IHM, EPERAM - Regulamento Interno», Abr-2017. [Em linha]. Disponível em: http://www.ihm.pt/images/img-regulamento/RegInt_IHM.pdf.

[59] IHM, EPERAM, «IHM, EPERAM - Missão, Visão e Valores», Mai-2015. [Em linha]. Disponível em: http://www.ihm.pt/index.php/ihm/missao-visao-e-valores.

[60] IHM, EPERAM, «IHM, EPERAM - Organograma», Jan-2018. [Em linha]. Disponível em: http://www.ihm.pt/index.php/ihm/organograma.

[61] ISO27K Forum, «ISMS Implementation and Certification Process», 2016. [Em linha]. Disponível em: http://www.iso27001security.com/ISO27k_ISMS_implementation_and_certification_process_v4.pdf.

[62] C. Oppenheim, J. Stenson, e R. M. S. Wilson, «Studies on Information as an Asset III: Views of Information Professionals», Journal of Information Science, UK, 2004, vol. 30, No. 2, pp. 181–190.

[63] D. Kim, M. G. Solomon, *Fundamentals of Information Systems Security*, Third edition, Jones & Barlett Learning, 2016

[64] P. Bowen, J. Hash, e M. Wilson, «NIST Special Publication 800-100 Information Security Handbook: A Guide for Managers», National Institute of Standards and Technology, Gaithersburg, MD, Out. 2006.

[65] Diário da República, *Resolução 41/2018, de 28 de março de 2018 - Requisitos técnicos mínimos das redes e sistemas para aplicação do RGPD*. 2018, pp. 1424–1430.

[66] I. de C. Peixinho, F. M. da Fonseca, e F. M. Lima, *Segurança de Redes e Sistemas*, Pedro Sangirardi. Rio de Janeiro: Escola Superior de Redes, 2013.

[67] National Institute of Standards and Technology, «National Vulnerability Database - Common Vulnerability Scoring System Calculator v3». [Em linha]. Disponível em: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

[68] Forum of Incident Security Response Teams, Inc. (FIRST), «Common Vulnerability Scoring System Version 3». [Em linha]. Disponível em: https://www.first.org/cvss/.

[69] SerNet Service Network GmbH, «Verinice. The Open Source ISMS tool», 2018. [Em linha]. Disponível em: https://verinice.com/en/product/#_product.

ANEXOS

Anexo I - Lista de normas da família 27000

Norma certificável	Publicada em	Descrição
ISO/IEC 27000	2018	*Information security management systems – Overview and vocabulary*
ISO/IEC 27001	2013	*Information security management systems – Requirements*.
Norma auxiliar	**Publicada em**	**Descrição**
ISO/IEC 27002	2013	*Code of practice for information security controls*
ISO/IEC 27003	2017	*Information security management system implementation guidance*
ISO/IEC 27004	2016	*Information security management – Monitoring, measurement, analysis and evaluation*
ISO/IEC 27005	2011	*Information security risk management*
ISO/IEC 27006	2015	*Requirements for bodies providing audit and certification of information security management systems*
ISO/IEC 27007	2017	*Guidelines for information security management systems auditing*
ISO/IEC TR 27008	2011	*Guidelines for auditors on information security controls*.
ISO/IEC 27009	2016	*Sector-specific application of ISO/IEC 27001 – Requirements*
ISO/IEC 27010	2015	*Information security management for inter-sector and inter-organizational communications*
ISO/IEC 27011	2016	*Information security management guidelines for telecommunications organizations based on* ISO/IEC 27002
ISO/IEC 27013	2015	*Guidance on the integrated implementation of* ISO/IEC 27001 *and* ISO/IEC 20000-1
ISO/IEC 27014	2013	*Governance of information security*
ISO/IEC TR 27016	2014	*Information security management – Organizational economics*
ISO/IEC 27017	2015	*Code of practice for information security controls based on* ISO/IEC 27002 *for cloud services*
ISO/IEC 27018	2014	*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
ISO/IEC TR 27019	2017	*Information security management guidelines based on* ISO/IEC 27002 *for process control systems specific to the energy utility industry*
ISO/IEC 27023	2015	*Mapping the revised editions of* ISO/IEC 27001 *and* ISO/IEC 27002
ISO/IEC 27031	2011	*Guidelines for information and communication technology readiness for business continuity*
ISO/IEC 27032	2012	*Guidelines for cybersecurity*
ISO/IEC 27033-1	2015	*Network security – Part 1: Overview and concepts*

Anexo I - Lista de normas da família 27000

Norma auxiliar	Publicada em	Descrição
ISO/IEC 27033-2	2012	*Network security – Part 2: Guidelines for the design and implementation of network security*
ISO/IEC 27033-3	2010	*Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues*
ISO/IEC 27033-4	2014	*Network security – Part 4: Securing communications between networks using security gateways*
ISO/IEC 27033-5	2013	*Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*
ISO/IEC 27033-6	2016	*Network security -- Part 6: Securing wireless IP network access*
ISO/IEC 27034-1	2011	*Application security – Part 1: Overview and concepts*
ISO/IEC 27034-2	2015	*Application security – Part 2: Organization normative framework for application security*
ISO/IEC 27035-1	2016	*Information security incident management – Part 1: Principles of incident management*
ISO/IEC 27035-2	2016	*Information security incident management – Part 2: Guidelines to plan and prepare for incident response*
ISO/IEC 27036-1	2014	*Information security for supplier relationships – Part 1: Overview and concepts*
ISO/IEC 27036-2	2014	*Information security for supplier relationships – Part 2: Requirements*
ISO/IEC 27036-3	2013	*Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*
ISO/IEC 27036-4	2016	*Information security for supplier relationships – Part 4: Guidelines for security of cloud services*
ISO/IEC 27037	2012	*Guidelines for identification, collection, acquisition and preservation of digital evidence*
ISO/IEC 27038	2014	*Specification for digital redaction*
ISO/IEC 27039	2015	*Selection, deployment and operations of intrusion detection systems (IDPS)*
ISO/IEC 27040	2015	*Storage security*
ISO/IEC 27041	2015	*Guidance on assuring suitability and adequacy of incident investigative methods*
ISO/IEC 27042	2015	*Guidelines for the analysis and interpretation of digital evidence*
ISO/IEC 27043	2015	*Incident investigation principles and processes*
ISO/IEC 27050-1	2016	*Electronic discovery – Part 1: Overview and concepts*
ISO 27799	2016	*Health informatics – Information security management in health using* ISO/IEC 27002

Anexo II - Quadro-resumo da estrutura das normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013

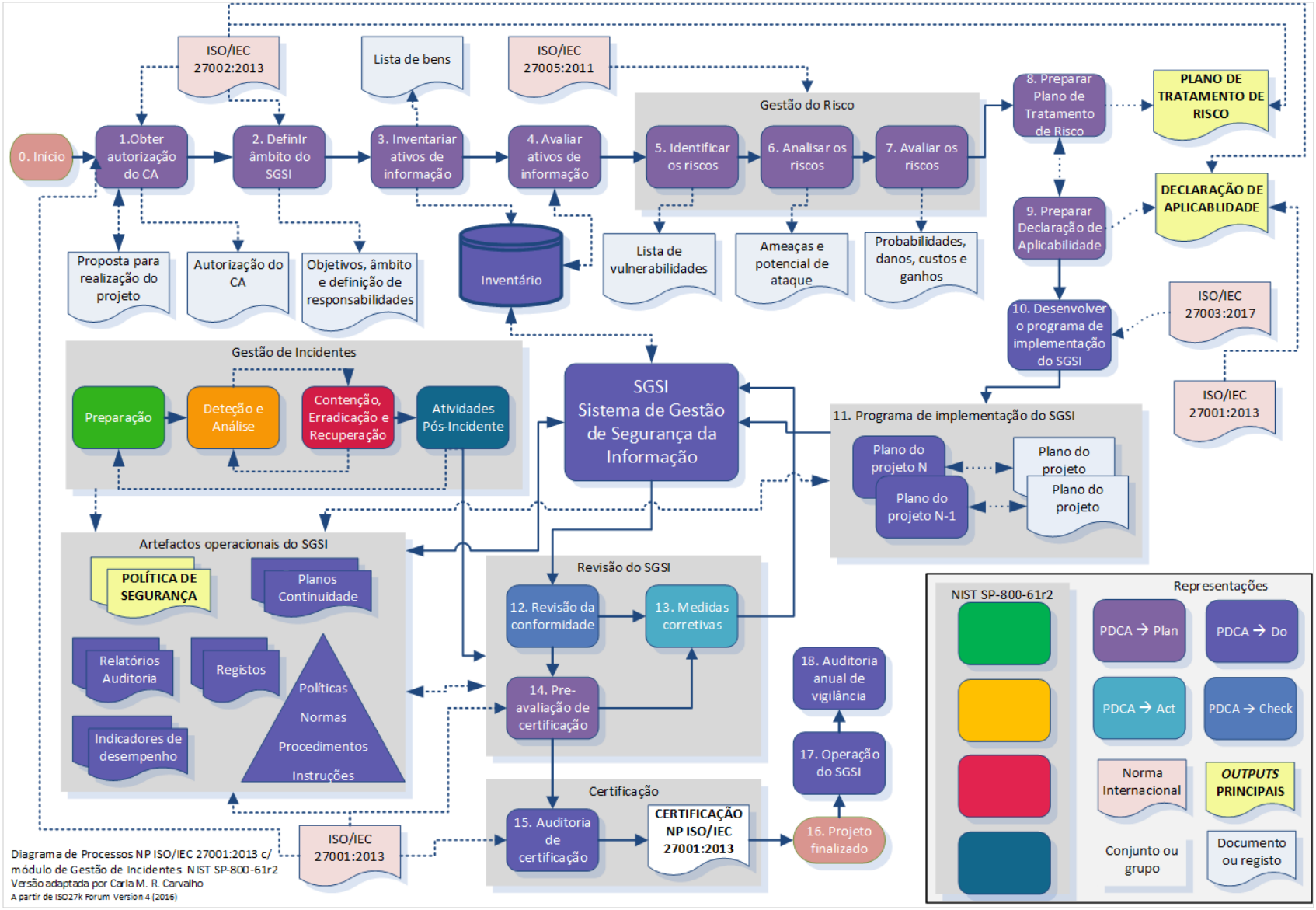
Secção	Controlo de referência	Categorias	Nº controlos
5 (*)	Políticas de segurança de informação	Diretrizes da gestão para segurança da informação	2
6	Organização de segurança de informação	Organização interna	7
		Dispositivos móveis e teletrabalho	
7	Segurança na gestão de recursos humanos	Antes da relação contratual	6
		Durante a relação contratual	
		Cessação e alteração da relação contratual	
8	Gestão de ativos	Responsabilidade pelos ativos	10
		Classificação da informação	
		Manuseamento de suporte de dados	
9	Controlo de acesso	Requisitos de negócio para controlo de acesso	14
		Gestão de acesso de utilizadores	
		Responsabilidades dos utilizadores	
		Controlo de acesso a sistemas e aplicações	
10	Criptografia	Controlos criptográficos	2
11	Segurança física e ambiental	Áreas seguras	15
		Equipamento	
12 (*)	Segurança de operações	Procedimentos e responsabilidades operacionais	14
		Proteção contra código malicioso	
		Salvaguarda de dados	
		Registos de eventos e monitorização	
		Controlo de software em sistemas de produção	
		Gestão de vulnerabilidades técnicas	
		Considerações para auditorias a sistemas de informação	

Anexo II - Quadro-resumo da estrutura das normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013

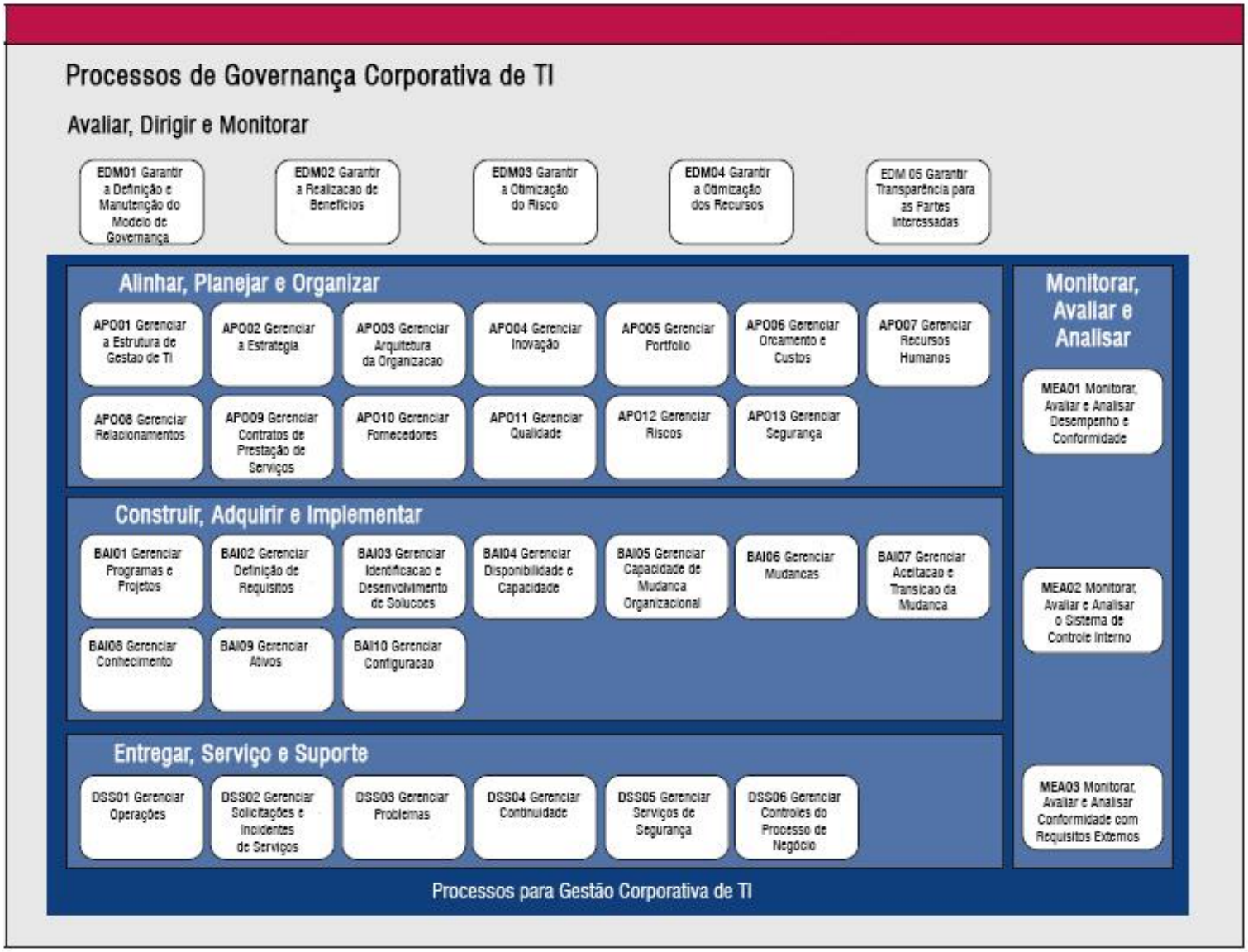
Secção	Controlo de referência	Categorias	Nº controlos
13 (*)	Segurança de comunicações	Gestão de segurança da rede	7
		Transferência de informação	
14	Aquisição, desenvolvimento e manutenção de sistemas	Requisitos de segurança de sistemas de informação	13
		Segurança no desenvolvimento e nos processos de suporte	
15	Relações com fornecedores	Segurança da informação nas relações com os fornecedores	5
		Gestão da entrega de serviços pelos fornecedores	
16 (*)	Gestão de incidentes de segurança da informação	Gestão de incidentes de segurança da informação e melhorias	7
17	Aspetos de segurança da informação na gestão da continuidade do negócio	Continuidade de segurança da informação	4
		Redundâncias	
18	Conformidade	Conformidade com requisitos legais e contratuais	8
		Revisões de segurança da informação	

(*) Secção implementada no projeto

Anexo III - Diagrama de Processos



Anexo IV - Modelo de referência de processo do COBIT 5



Anexo V - Funções e Responsabilidades (Anexo B da ISO 27003:2010)

Função	Existe na IHM	Responsabilidade
Conselho de Administração	**Sim**	Visão, decisões estratégicas e coordenação de atividades de direção e controlo da empresa. Responsável final pela segurança da informação.
Diretor de serviço	**Sim**	Responsável pelas funções organizacionais.
Diretor de Segurança da Informação (CISO)	**Não**	Responsável pela governança e gestão da segurança da informação, assegura o correto tratamento dos ativos de informação.
Chefe de serviço	**Sim**	Responsável pelas funções operacionais.
Comissão de Segurança da Informação (membro da)	**Não**	Lida com os recursos da informação e tem um papel de liderança no Sistema de Gestão de Segurança da Informação (SGSI).
Equipa de Planeamento de Segurança da Informação (membro da)	**Não**	Para as operações durante o estabelecimento do SGSI, trabalha nos serviços e resolve conflitos até que este seja estabelecido.
Partes interessadas	**Sim**	Entidades que não operam na empresa, mas com interesse nesta, tais como clientes, fornecedores, parceiros, entidades associadas, entidades governamentais e outras.
Gestor de tecnologia de informação	**Sim**	Gere todos os recursos de tecnologia de informação.
Administrador de sistema(s)	**Sim**	Responsável por um ou mais sistemas de informação.
Gestor das instalações	**Sim**	Responsável pela segurança física das instalações.
Gestor de risco	**Não**	Responsável pela gestão do risco da empresa. Realiza a avaliação, tratamento e monitorização do risco.
Consultor jurídico	**Sim**	Lida com os aspetos legais relacionados com os riscos de segurança da informação.
Gestor de recursos humanos	**Sim**	Detém a responsabilidade global sobre a equipa.
Arquivista	**Sim**	Responsável pela segurança do armazenamento de informações vitais.
Encarregado de proteção de dados	**Não**	Imposto pelo RGPD, é responsável pela supervisão dos mecanismos para a segurança dos dados pessoais e questões de privacidade relacionadas.
Especialista	**Sim**	Responsável por algumas operações na empresa, deve ser referido em relação à ação que desempenha no SGSI.

Anexo VI - Identificação e Análise de Ameaças

Tipo	Ameaça	Fonte (*)	Probabilidade / Impacto
Evento Natural	Sismo	N	4/7
	Aluvião	N	4/7
	Fenómeno meteorológico	N	4/7
	Terramoto	N	3/9
	Tsunami	N	2/10
Calamidade	Guerra nuclear	I	2/10
Ameaça física	Incêndio	A, I, N	3/8
	Inundação	A, I, N	3/8
	Poluição	A, I, N	3/8
	Corte ou sobrecarga de corrente	A, I, N	6/3
	Sabotagem	A, I	6/4
	Vandalismo	A, I	5/4
	Acidente com equipamento	A, I	7/3
	Corte na rede local de dados	A, I	6/4
	Corte no acesso à Internet	A, I	6/4
	Acesso físico não autorizado	I	7/7
Ação não autorizada	Utilização não autorizada de equipamento	I	5/3
	Destruição de equipamento	I	4/5
	Instalação não autorizada de *software*	I	5/6
	Utilização não autorizada de *software*	I	5/4
	Apropriação indevida de informação	I	8/4
	Acesso não autorizado ao sistema de informação	I	7/4
	Utilização indevida das ferramentas de auditoria	I	4/4
	Obtenção de cópias ilegais de software	I	5/7
	Utilização de cópias de software falsificadas ou ilegais	A, I	6/7
	Processamento ilegal de dados	I	6/4
	Comprometimento dos dados	I	6/6

Anexo VI - Identificação e Análise de Ameaças

Tipo	Ameaça	Fonte (*)	Probabilidade / Impacto
	Dados de fontes não confiáveis	A, I	8/7
Comprometimento da informação	Danos resultantes de testes de penetração	A, I	5/6
	Destruição de registos	A, I	5/7
	Determinação de localização	I	6/4
	Divulgação de palavras-chave	A, I	6/6
	Divulgação não autorizada	A, I	7/4
	Engenharia social	I	6/7
	Espionagem	I	5/4
	Fraude	I	6/5
	Furto	A, I	5/5
	Escutas (*sniffing*)	I	6/2
	Vírus	A, I	7/4
	Violação de propriedade intelectual	A, I	8/5
Falha técnica	Defeito de equipamento	A	5/4
	Erros de software	A	9/1
	Falha de equipamento	A	6/3
	Falha de equipamento de comunicação	A	4/7
	Saturação do sistema de informação	A, I	5/5
	Quebra da capacidade de manutenção do sistema de informação	A, I	5/6
Comprometimento de funções	Erros humanos	A, I	9/3
	Abuso de privilégios	A, I	6/5
	Repúdio de ações	I	6/5
	Indisponibilidade de recursos humanos	A, I, N	6/5

- (*) Fonte: A(acidental), I (intencional) ou N (natural)

Anexo VII – Plano de Tratamento do Risco

PLANO DE TRATAMENTO DO RISCO Válido a partir de: **dd/mm/aaaa**

Editor: _____ **Última versão aprovada:** _____
Aprovador: _____ **Data de aprovação:** _____
Versão: _____ **Estado (Em edição / Aprovado):** _____

A.5 - POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO															
Ameaça	**Confidencialidade**	**Integridade**	**Disponibilidade**	**Probabilidade**	**Impacto**	**Nível do Risco**	**Controlo a implementar**	**Descrição do controlo**	**Detalhe da implementação**	**Prioridade de intervenção**	**Quem implementa**	**Data alvo**	**Prazo Intervenção**	**Custo de implementação**	**Observações**
Utilização arbitrária de recursos informáticos e da informação	X	X	X	8	7	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Segurança da Informação**, que especifique as regras e princípios para a segurança da informação, seja qual for o seu formato, a forma como é partilhada, comunicada ou armazenada.	Prioritária	Chefia Informática		Imediato		
Acesso indevido a informação por má classificação	X	-	-	6	6	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Classificação da Informação**, que especifique a classificação a atribuir à informação digital produzida.	Prioritária	Chefia Informática		Imediato		
Impossibilidade de reposição de backup por falha de integridade	-	X	X	5	9	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Cópia de Segurança**, que especifique a realização de backups e a sua verificação.	Prioritária	Chefia Informática		Imediato		
Divulgação de informação confidencial	X	-	-	7	3	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Confidencialidade da Informação**, que especifique o tratamento dos dados confidenciais.	Prioritária	Chefia Informática		Imediato		
Acesso indevido de terceiros a informação interna	X	-	-	6	6	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Controlo de Acesso**, que especifique as regras de acesso aos sistemas, o registo de utilizadores e a gestão de direitos de acesso.	Prioritária	Chefia Informática		Imediato		
Receção de e-mails adulterados (phishing)	X	X	X	6	7	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Correio Eletrónico**, que especifique as regras para utilização do sistema de e-mail de forma global (incluir as aplicações desktop/webmail, acesso a contas externas, envio/receção de anexos, assinatura digital, ...).	Prioritária	Chefia Informática		Imediato		
Erros na submissão de dados por falta de validação server-side	X	-	X	7	5	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Desenvolvimento Aplicacional**, que especifique as regras para o desenvolvimento seguro de software, as linguagens e metodologias a adotar, o controlo de versões, os testes de segurança e de aceitação e a documentação a produzir.	Prioritária	Chefia Informática		Imediato		
Furto de equipamento móvel contendo dados confidenciais	X	-	X	7	6	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Dispositivos Móveis**, que especifique a utilização de portáteis, tablets, smartphones e outros dispositivos móveis para tratamento de dados da IHM.	Prioritária	Chefia Informática		Imediato		
Comunicação de dados sensíveis em texto livre	X	-	-	8	6	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Encriptação**, que especifique a utilização de mecanismos de encriptação para salvaguarda da confidencialidade e integridade da informação transmitida e armazenada.	Prioritária	Chefia Informática		Imediato		
Injeção massiva de dados na rede via streaming online	-	-	X	9	6	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Navegação na Web**, que especifique o acesso a web sites e a conteúdos descarregáveis.	Prioritária	Chefia Informática		Imediato		

Anexo VII – Plano de Tratamento do Risco

A.5 - POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO																
Ameaça	**Confidencialidade**	**Integridade**	**Disponibilidade**	**Probabilidade**	**Impacto**	**Nível do Risco**	**Controlo a implementar**	**Descrição do controlo**	**Detalhe da implementação**	**Prioridade de intervenção**	**Quem implementa**	**Data alvo**	**Prazo Intervenção**	**Custo de implementação**	**Observações**
Acesso indevido através de palavra-passe fraca	X	-	-	8	5	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Palavra-passe**, que especifique os critérios para a criação de palavras-passe seguras.	Prioritária	Chefia Informática		Imediato		
Ataque através de ransomware	-	X	X	5	8	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Gestão de Incidentes de Segurança**, que especifique os incidentes que podem afetar a segurança e a integridade dos ativos de informação e quais as medidas a tomar caso ocorram.	Prioritária	Chefia Informática		Imediato		
Vírus	X	X	X	5	6	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Instalação de Software**, que especifique as aplicações que podem ser instaladas e quem pode instalar.	Prioritária	Chefia Informática		Imediato		
Exploração de serviços na firewall	-	-	X	6	5	Médio	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Segurança de Rede**, que defina as regras para a segurança na rede (incluir firewall, routers, switches, logs, serviços de rede, palavras-passe dos dispositivos de rede, testes de segurança, ...).	Prioritária	Chefia Informática		Imediato		
Acesso a zonas críticas de comunicações e processamento de dados	X	X	X	8	7	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Segurança Física**, que especifique os controlos de acesso físico às instalações e os mecanismos de proteção dos recursos físicos.	Prioritária	Chefia Informática		Imediato		
Transferência não controlada de informação para equipamentos pessoais	X	-	-	7	5	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Teletrabalho**, que especifique as regras de acesso remoto aos recursos informáticos da empresa.	Prioritária	Chefia Informática		Imediato		
Acesso indevido a informação	X	X	-	6	5	Elevado	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Transferência de Informação**, que especifique as regras de acesso remoto ao posto de trabalho para execução de tarefas profissionais.	Prioritária	Chefia Informática		Imediato		
Danos à reputação da empresa por publicação de informação confidencial	X	X	X	4	5	Médio	**A.5.1.1**	Políticas para a segurança da informação	Estabelecer uma **Política de Utilização de Redes Sociais**, que especifique as regras para partilha de conteúdos proprietários da empresa, resposta a clientes e comentários de natureza profissional.	Agendada	Chefia Informática		1-2 meses		

Anexo VII – Plano de Tratamento do Risco

PLANO DE TRATAMENTO DO RISCO Válido a partir de: **dd/mm/aaaa**

Editor: _____ **Última versão aprovada:** _____
Aprovador: _____ **Data de aprovação:** _____
Versão: _____ **Estado (Em edição / Aprovado):** _____

A.12 - SEGURANÇA DE OPERAÇÕES															
Ameaça	**Confidencialidade**	**Integridade**	**Disponibilidade**	**Probabilidade**	**Impacto**	**Nível do Risco**	**Controlo a implementar**	**Descrição do controlo**	**Detalhe da implementação**	**Prioridade de intervenção**	**Quem implementa**	**Data alvo**	**Prazo Intervenção**	**Custo de implementação**	**Observações**
Danos resultantes de má utilização dos sistemas	-	X	-	5	6	Elevado	**A.12.1.1**	Procedimentos de operação documentados	Documentar os procedimentos de operação dos sistemas.	Prioritária	Equipa Informática		Imediato		
Acesso e privilégios insuficientes ou excessivos por alterações na estrutura orgânica	X	-	X	5	5	Médio	**A.12.1.2**	Gestão de alterações	Rever todos os direitos de acesso aos sistemas e privilégios nas aplicações.	Prioritária	Equipa Informática		Imediato		
Falha no sistema por falta de espaço em disco	-	-	X	4	5	Médio	**A.12.1.3**	Gestão da capacidade	Monitorizar o armazenamento, estimar o crescimento do volume de dados e antecipar a operação de expansão da capacidade.	Agendada	Equipa Informática		1-2 meses		
Danos em aplicações em ambiente de produção	-	X	-	5	6	Elevado	**A.12.1.4**	Separação entre ambientes de desenvolvimento, teste e de produção	Realizar os testes de desenvolvimento em ambiente de laboratório ou de simulação.	Prioritária	Equipa Informática		Imediato		
Engenharia social	X	X	X	6	7	Elevado	**A.12.2.1**	Controlos contra código malicioso	Implementar sistema de e-mail com filtros anti-spam.	Prioritária	Equipa Informática		Imediato		E.g. phishing
Vírus	-	-	X	7	4	Elevado	**A.12.2.1**	Controlos contra código malicioso	Implementar solução antivirus com segurança preventiva contra ataques zero-day.	Prioritária	Equipa Informática		Imediato		
Destruição de registos	-	-	X	5	7	Elevado	**A.12.3.1**	Salvaguarda de informação	Realizar e testes regulares de cópias de segurança de informação, software e imagens de sistema.	Prioritária	Equipa Informática		Imediato		
Repúdio de ação não autorizada	X	X	X	4	3	Residual	**A.12.4.1**	Registos de eventos	Atribuir aos técnicos a tarefa de produzir registos de todas as atividades realizadas em complemento aos logs nos sistemas.	Não Prioritária	Chefia Informática		3-6 meses		
Alteração indevida de registos	-	X	-	5	4	Médio	**A.12.4.2**	Proteção da informação registada	Proibir conta de utilizador partilhada com privilégios de administração.	Agendada	Chefia Informática		1-2 meses		
Realização de atividades não programadas cuja segurança não foi validada	X	X	X	6	5	Elevado	**A.12.4.3**	Registos de administrador e de operador	Atribuir a tarefa de registar todas as atividades realizadas a todo o pessoal informático indicando claramente a sua identificação.	Prioritária	Chefia Informática		Imediato		
Impossibilidade de registo por indicação de tempo futuro	-	-	X	4	3	Baixo	**A.12.4.4**	Sincronização de relógio	Sincronizar todos os sistemas para o mesmo servidor de hora	Não Prioritária	Equipa Informática		3-6 meses		Sincronização com sistemas da LCRAM
Instalação não autorizada de software	-	X	-	5	6	Elevado	**A.12.5.1**	Instalação de software nos sistemas de produção	Registar todas as instalações efetuadas, o respetivo nº de licença, os postos e utilizadores do software e fundamentar a instalação.	Prioritária	Equipa Informática		Imediato		
Intrusão por vulnerabilidade não tratada (patch não aplicado)	X	X	X	7	7	Elevado	**A.12.6.1**	Gestão de vulnerabilidades técnicas	Registar imediatamente todas as vulnerabilidades detetadas, estimando o impacto e decidir o(s) controlo(s) a aplicar.	Prioritária	Chefia Informática / Equipa Informática		Imediato		
Inconformidade legal por falta de licenciamento	-	X	-	5	6	Elevado	**A.12.6.2**	Restrições sobre a instalação de software	Instalar apenas software legítimo, licenciado e autorizado superiormente.	Prioritária	Equipa Informática		Imediato		
Não deteção de ações não autorizadas	-	X	-	5	5	Elevado	**A.12.7.1**	Controlos de auditoria nos sistemas de informação	Agendar auditorias periódicas a todos os sistemas, em horário pós-laborar.	Prioritária	Chefia Informática		Imediato		

Anexo VII – Plano de Tratamento do Risco

PLANO DE TRATAMENTO DO RISCO

Válido a partir de: **dd/mm/aaaa**

Editor: _____
Aprovador: _____
Versão: _____

Última versão aprovada: _____
Data de aprovação: _____
Estado (Em edição / Aprovado): _____

A.13 - SEGURANÇA DE COMUNICAÇÕES															
Ameaça	**Confidencialidade**	**Integridade**	**Disponibilidade**	**Probabilidade**	**Impacto**	**Nível do Risco**	**Controlo a implementar**	**Descrição do controlo**	**Detalhe da implementação**	**Prioridade de intervenção**	**Quem implementa**	**Data alvo**	**Prazo Intervenção**	**Custo de implementação**	**Observações**
Spoofing nas respostas ARP a pedidos	-	X	X	5	4	Médio	**A.13.1.1**	Controlos da rede	Hard-code entradas ARP	Agendada	Equipa Informática		1-2 meses		Para impedir spoofing nas respostas ARP a pedidos e evitar ARP cache poisoning.
Ocorrência de comunicações não autorizadas e não monitorizadas	X	-	-	7	2	Médio	**A.13.1.2**	Segurança de serviços de rede	Desativar todos os serviços de rede que não são necessários.	Agendada	Equipa Informática		1-2 meses		E.g. IPv6 link-local address em AUTO pode comunicar sem que o admin se aperceba.
Acesso indevido a recursos no mesmo segmento de rede	X	X	X	6	4	Elevado	**A.13.1.3**	Segregação das redes	Planear e implementar VLANs para separação das comunicações	Prioritária	Equipa Informática		Imediata		
Captura de dados em operações online	X	-	-	5	4	Médio	**A.13.2.1**	Políticas e procedimentos de transferência de informação	Implementar HTTPS em todos os servidores web	Agendada	Equipa Informática		1-2 meses		Transfere os dados encriptados via SSL/TLS.
Repúdio sobre falhas de integridade nos dados após as comunicações estabelecidas	X	-	-	4	4	Médio	**A.13.2.2**	Acordos sobre transferência de informação	Estabelecer protocolos com entidades externas (Governo Regional, SIBS, bancos, fornecedores, ...) para transferência segura de dados	Agendada	Equipa Informática		1-2 meses		
Repúdio sobre envio de e-mail	X	X	-	5	6	Elevado	**A.13.2.3**	Mensagens eletrónicas	Assinar digitalmente (Cartão do Cidadão) todos os e-mails a enviar	Prioritária	Equipa Informática		Imediato		Leitor de cartões para todos os colaboradores
Engenharia social	X	X	X	6	7	Elevado	**A.13.2.4**	Acordos de confidencialidade ou de	Proibir a divulgação de informação através de canais não autorizados.	Prioritária	Equipa Informática		Imediato		
Engenharia social	X	X	X	6	7	Elevado	**A.13.2.4**	Acordos de confidencialidade ou de	Escrutinar a informação a divulgar online.	Prioritária	Equipa Informática		Imediato		
Divulgação não autorizada	X	-	-	7	4	Elevado	A.13.2.4	Acordos de confidencialidade ou de não divulgação	Rever e atualizar os requisitos para os acordos de confidencialidade ou de não divulgação de informação sempre que evoluções a nível da segurança tecnológicas o exijam.	Prioritária	Equipa Informática		Imediato		

Anexo VII – Plano de Tratamento do Risco

PLANO DE TRATAMENTO DO RISCO

Válido a partir de: **dd/mm/aaaa**

Editor: _____
Aprovador: _____
Versão: _____

Última versão aprovada: _____
Data de aprovação: _____
Estado (Em edição / Aprovado): _____

A.16 - GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO															
Ameaça	**Confidencialidade**	**Integridade**	**Disponibilidade**	**Probabilidade**	**Impacto**	**Nível do Risco**	**Controlo a implementar**	**Descrição do controlo**	**Detalhe da implementação**	**Prioridade de intervenção**	**Quem implementa**	**Data alvo**	**Prazo Intervenção**	**Custo de implementação**	**Observações**
Caos na gestão de cenários de crise	-	-	X	5	5	Elevado	**A.16.1.1**	Responsabilidades e procedimentos	Estabelecer plano de resposta a incidentes, definindo procedimentos, intervenientes e responsabilidades.	Prioritária	Chefia Informática		Imediato		
Continuação de cenário de ataque	X	X	X	5	5	Elevado	**A.16.1.2**	Reportar eventos de segurança da informação	Definir os canais de gestão para reporte de eventos de segurança.	Prioritária	Chefia Informática		Imediato		
Continuação de cenário de ataque	X	X	X	5	5	Elevado	**A.16.1.2**	Reportar eventos de segurança da informação	Instruir técnicos e prestadores de serviços para reportarem imediatamente qualquer evento de segurança através dos canais definidos para o efeito.	Prioritária	Chefia Informática		Imediato		
Exploração de vulnerabilidade	X	X	X	7	4	Elevado	**A.16.1.3**	Reportar pontos fracos de segurança da informação	Instruir técnicos e prestadores de serviços para reportarem toda e qualquer vulnerabilidade detetada nos sistemas ou serviços.	Prioritária	Chefia Informática		Imediato		
Continuação de cenário de ataque	X	X	X	6	5	Elevado	**A.16.1.4**	Avaliação e decisão sobre eventos de segurança da informação	Estabelecer plano de classificação de eventos de segurança indicando quais os que são incidentes.	Prioritária	Chefia Informática		Imediato		
Resposta insuficiente para mitigar o incidente	X	X	X	6	5	Elevado	**A.16.1.5**	Resposta a incidentes de segurança da informação	Responder a incidentes de acordo com o plano de resposta estabelecido.	Prioritária	Chefia Informática		Imediato		
Resposta insuficiente para mitigar o incidente	X	X	X	6	5	Elevado	**A.16.1.6**	Aprender com os incidentes de segurança da informação	Reavaliar e ajustar o plano de resposta a incidentes de forma a incluir o conhecimento obtido em eventuais ocorrências.	Prioritária	Chefia Informática		Imediato		
Perda de conhecimento sobre osataque realizado	X	X	X	6	5	Elevado	**A.16.1.7**	Recolha de evidências	Isolar e preservar os equipamentos efetados por incidentes para recolha de prova.	Prioritária	Chefia Informática		Imediato		

Anexo VIII - Declaração de Aplicabilidade

DECLARAÇÃO DE APLICABILIDADE Válida a partir de: **dd/mm/aaaa**

Legenda:

RL: **requisitos legais**, OC: **obrigações contratuais**, RN/MP: **requisitos de negócio / melhores práticas**, RAR: **resultado da avaliação de risco**, EC: **em curso**, N/A: **não aplicável**

Anexo A da norma NP ISO/IEC 27001:2013			Controlo existente	Controlo a aplicar	Descrição e justificação, inclusive para as exclusões, quando aplicável	Motivos para a seleção					Recursos associados	Data implementação	Resumo da implementação (o que fazer e como fazer)	Responsável	Prazo de conclusão
						RL	OC	RN/MP	RAR	N/A					
Secção	Objetivo de controlo / Controlo														
	5.1	Diretrizes da gestão para a segurança da informação													
	5.1.1	Estabelecer uma Política de Aceitação	Não	Sim	Especifica a utilização aceitável dos recursos informáticos através de um conjunto de políticas de segurança. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir a designação [Pol 001/IHM].	CA; Chefia Informática;	
	5.1.1	Estabelecer uma Política de Classificação da Informação	Sim	Sim	Especifica a classificação a atribuir à informação digital produzida. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Plano de classificação aprovado aquando da implementação do sistema de gestão documental (Gescor). Publicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 002/IHM].	CA; Chefia Informática;	
	5.1.1	Estabelecer uma Política de Cópia de Segurança	Não	Sim	Especifica a realização de backups e a sua verificação. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Equipa Informática		Definir o software a utilizar, os objetos alvo de backup, a agenda de execução (dias da semana e hora), a periodicidade, o repositório de armazenamento, os testes de verificação de integridade e as responsabilidades. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir a designação [Pol 003/IHM].	CA; Chefia Informática;	
	5.1.1	Estabelecer uma Política de Confidencialidade da Informação	Não	Sim	Especifica o tratamento dos dados confidenciais. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Critérios de confidencialidade aprovados aquando da implementação do sistema de gestão documental (Gescor). Rever confidencialidade dos ficheiros partilhados e nas aplicações (pseudonimização). Criar perfis em todas as aplicações. Publicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 004/IHM].	CA; Chefia Informática;	

Anexo VIII - Declaração de Aplicabilidade

Anexo A da norma NP ISO/IEC 27001:2013		Controlo existente	Controlo a aplicar	Descrição e justificação, inclusive para as exclusões, quando aplicável	Motivos para a seleção					Recursos associados	Data implementação	Resumo da implementação (o que fazer e como fazer)	Responsável	Prazo de conclusão
					RL	OC	RN/MP	RAR	RJA					
Secção	Objetivo de controlo / Controlo													
	5.1.1 Estabelecer uma Política de Controlo de Acesso	Não	Sim	Especifica as regras de acesso às redes, o registo de utilizadores e a gestão de direitos de acesso. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Definir quem pode aceder às redes, quais os equipamentos permitidos, os requisitos para registo de utilizadores e os perfis a atribuir. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 005/IHM].	CA; Chefia Informática;	
	5.1.1 Estabelecer uma Política de Correio Eletrónico	Não	Sim	Especifica as regras para utilização do sistema de e-mail. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Definir as aplicações desktop/webmail autorizadas, as regras de acesso a contas externas, o tipo de anexos permitidos e a inclusão de assinatura digital. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 006/IHM].	CA; Chefia Informática;	
	5.1.1 Estabelecer uma Política de Desenvolvimento Aplicacional	Não	Sim	Especifica as regras para o desenvolvimento seguro de software. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Equipa Informática		Definir as linguagens autorizadas, as metodologias a adotar, o controlo de versões, os testes de segurança e de aceitação, e a documentação a produzir. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 007/IHM].	CA; Chefia Informática;	
	5.1.1 Estabelecer uma Política de Dispositivos Móveis	Não	Sim	Especifica a utilização de portáteis, tablets, smartphones e outros dispositivos móveis para tratamento de dados da IHM. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Definir medidas de segurança que mitiguem os riscos associados à utilização destes equipamentos. Decidir a permissão/bloqueio de Unidades Móveis de Armazenamento USB (Pen Drive). Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 008/IHM].	CA; Chefia Informática;	

Anexo VIII - Declaração de Aplicabilidade

Anexo A da norma NP ISO/IEC 27001:2013			Controlo existente	Controlo a aplicar	Descrição e justificação, inclusive para as exclusões, quando aplicável	Motivos para a seleção					Recursos associados	Data implementação	Resumo da implementação (o que fazer e como fazer)	Responsável	Prazo de conclusão
						RL	OC	RN/MP	RAR	RVA					
Secção	Objetivo de controlo / Controlo														
A.5: Políticas de segurança da informação	5.1.1	Estabelecer uma Política de Encriptação	Não	Sim	Especifica a utilização de mecanismos de encriptação para salvaguarda da confidencialidade e integridade da informação transmitida e armazenada. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Definir quais os controlos criptográficos a utilizar, as aplicações afetadas, os protocolos a utilizar e os mecanismos para segurança de chaves criptográficas. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 009/IHM].	CA; Chefia Informática;	
	5.1.1	Estabelecer uma Política de Gestão de Ativos	Não	Sim	Especifica os mecanismos para identificação de ativos e as responsabilidades de segurança adequadas. RN/MP para conformidade com o RGPD.	-	-	X	X		Equipamentos, utilizadores:		Registar inventário de ativos, identificar os responsáveis por cada ativo e as regras para utilização aceitável e devolução dos ativos. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 010/IHM].	CA; Chefia Informática;	
	5.1.1	Estabelecer uma Política de Gestão de Incidentes de Segurança da Informação	Não	Sim	Especifica os incidentes que podem afetar a segurança e a integridade dos ativos de informação e quais as medidas a tomar caso ocorram. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Definir os critérios de decisão sobre a natureza de um evento de segurança (i.e., se é um incidente ou não). Listar incidentes típicos e quais as medidas a tomar. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 011/IHM].	CA; Chefia Informática;	
	5.1.1	Estabelecer uma Política de Instalação de Software	Não	Sim	Especifica as regras para instalação de software nos sistemas. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-			Definir os critérios para a instalação de software nos sistemas. Listar software permitido, responsabilidades de instalação e informação sobre o licenciamento. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 012/IHM].	CA; Chefia Informática;	

Anexo VIII - Declaração de Aplicabilidade

Anexo A da norma NP ISO/IEC 27001:2013		Controlo existente	Controlo a aplicar	Descrição e justificação, inclusive para as exclusões, quando aplicável	Motivos para a seleção					Recursos associados	Data implementação	Resumo da implementação (o que fazer e como fazer)	Responsável	Prazo de conclusão
					RL	OC	RN/MP	RAR	MA					
Secção	Objetivo de controlo / Controlo													
	5.1.1 Estabelecer uma Política de Navegação na Web	Não	Sim	Especifica o acesso a websites e a conteúdos descarregáveis. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Definir quais as categorias de página permitidas/bloqueadas. Definir permissões para download de conteúdos da web. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 013/IHM].	CA; Chefia Informática;	
	5.1.1 Estabelecer uma Política de Palavra-passe	Não	Sim	Especifica os critérios para a criação de palavras-passe seguras. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Definir o método de construção de palavras-passe seguras, o n.º mínimo e o tipo de caracteres. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 014/IHM].	CA; Chefia Informática;	
	5.1.1 Estabelecer uma Política de Segurança de Rede	Não	Sim	Define as especificações técnicas e os controlos necessários para a segurança na rede. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Equipa Informática		Definir os controlos a implementar e os protocolos a utilizar na firewall, nos routers e switches, os logs a obter, as palavras-passe dos dispositivos de rede e os testes de segurança a efetuar. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 015/IHM].	CA; Chefia Informática;	
	5.1.1 Estabelecer uma Política de Segurança Física	Não	Sim	Especifica os controlos de acesso físico às instalações e os mecanismos de proteção dos recursos físicos. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Definir medidas de proteção física dos equipamentos, das zonas críticas e os controlos de acesso físico (quem pode aceder). Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 016/IHM].	CA; Chefia Informática;	

Anexo VIII - Declaração de Aplicabilidade

Anexo A da norma NP ISO/IEC 27001:2013			Controlo existente	Controlo a aplicar	Descrição e justificação, inclusive para as exclusões, quando aplicável	Motivos para a seleção					Recursos associados	Data implementação	Resumo da implementação (o que fazer e como fazer)	Responsável	Prazo de conclusão
						RL	OC	RN/MP	RAR	RCA					
Secção	Objetivo de controlo / Controlo														
	5.1.1	Estabelecer uma Política de Teletrabalho	Não	Sim	Especifica as regras de acesso remoto ao posto de trabalho para execução de tarefas profissionais. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Definir o software para teletrabalho, quem pode aceder e a permissão/proibição de transferência de ficheiros. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 017/IHM].	CA; Chefia Informática;	
	5.1.1	Estabelecer uma Política de Transferência de Informação	Não	Sim	Especifica as regras para transferência de informação através de qualquer meio de comunicação. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Equipa Informática		Implementar HTTPS em serviços a disponibilizar na web. Encriptar e-mails e ficheiros a transferir pela internet. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 018/IHM].	CA; Chefia Informática;	
	5.1.1	Estabelecer uma Política de Utilização de Redes Sociais	Não	Sim	Especifica as regras para partilha de conteúdos proprietários da empresa, resposta a clientes e comentários de natureza profissional. RL, OC e RN/MP para conformidade com o RGPD.	X	X	X	X	-	Todos os recursos humanos		Especificar quais os conteúdos proprietários passíveis de publicação, os direitos sobre as imagens, os consetimentos a obter em caso de fotos com pessoas, o critério de resposta a comentários por parte da IHM, e as regras para comentários profissionais por parte dos colaboradores. Definir, aprovar, publicar e comunicar o documento que inclui o resumo (i.e., objetivo da política), o âmbito (i.e., alcance da política), a política (i.e., detalhe sobre o conteúdo), a aplicação (i.e., requisitos) e o histórico de revisões (i.e., registo da evolução da política). Atribuir designação [Pol 019/IHM].	CA; Chefia Informática;	
	5.1.2	Rever as políticas de segurança da informação	Não	Sim	Revisão das políticas em vigor.	-	-	X	-	-	Todos os recursos humanos		Rever as políticas periodicamente (1x por ano ou bienal) ou sempre que estejam previstas alterações significativas.	CA; Chefia Informática;	
	12.1	**Procedimentos e responsabilidades operacionais**													
	12.1.1	Procedimentos de operação documentados	Não	Sim	Documentar os procedimentos de operação dos sistemas e aplicações para os utilizadores.	-	-	X	X	-	Sistemas, aplicações;		Disponibilizar manuais do utilizador e tutoriais específicos sobre o sistema operativo e aplicações em utilização na IHM.	Equipa Informática	

Anexo VIII - Declaração de Aplicabilidade

Anexo A da norma NP ISO/IEC 27001:2013			Controlo existente	Controlo a aplicar	Descrição e justificação, inclusive para as exclusões, quando aplicável	Motivos para a seleção					Recursos associados	Data implementação	Resumo da implementação (o que fazer e como fazer)	Responsável	Prazo de conclusão
						RL	OC	RN/MP	RAR	RCA					
Secção	**Objetivo de controlo / Controlo**														
A.12: Segurança de operações	12.1.1	Procedimentos de operação documentados	Não	Sim	Documentar os procedimentos de operação e configuração dos sistemas e aplicações para a equipa informática.	-	-	X	X	-	Sistemas, aplicações;		Desenvolvimento de uma Knowledge Base (fórum) para publicação de procedimentos de operação e configuração sobre os sistemas e aplicações em utilização na IHM.	Equipa Informática	
	12.1.1	Procedimentos de operação documentados	Não	Sim	Documentar os procedimentos para realização de testes aos sistemas, aplicações e rede para a equipa informática.	-	-	X	X	-	Sistemas, aplicações;		Detalhar todos os passos a realizar, indicar resultados previstos (negativos/positivos), calendarizar e definir as responsabilidades.	Equipa Informática	
	12.1.2	Gestão de alterações	Sim	Sim	Rever todos os direitos de acesso aos sistemas e privilégios nas aplicações em caso de alterações à estrutura orgânica.	-	-	X	X	-	Sistemas, aplicações, utilizadores;		Identificar os utilizadores nas Unidades Orgânicas alteradas e rever os direitos atribuídos.	Equipa Informática	
	12.1.2	Gestão de alterações	Sim	Sim	Analisar o impacto das alterações aos processos de negócio na segurança dos sistemas, na capacidade de processamento e nos procedimentos executados para correta adaptação.	X	X	X	X	-	Sistemas, aplicações, utilizadores;		Especificar todas as alterações e identificar as adaptações de segurança necessárias aos sistemas.	Equipa Informática	
	12.1.2	Gestão de alterações	Sim	Sim	Proceder aos ajustamentos que os novos processos requerem atendendo à análise de impacto efetuada.	X	X	X	X	-	Sistemas, aplicações, utilizadores;		Executar backup antes de qualquer alteração. Proceder às novas parametrizações e realizar testes antes da reentrada em produção.	Equipa Informática	
	12.1.3	Gestão de capacidade	Sim	Sim	Garantir que a capacidade dos sistemas é ajustada aos requisitos para o seu bom funcionamento.	X	-	X	X	-	Sistemas		Examinar a capacidade de cada sistema (CPU, memória, disco, rede, capacidade gráfica) face ao desempenho desejado.	Equipa Informática	
	12.1.4	Separação entre ambientes de desenvolvimento, teste e de produção	Não	Sim	Garantir a separação entre os ambientes de desenvolvimento, de teste e de produção.	X	-	X	X	-	Sistemas, aplicações, utilizadores;		Garantir ambiente de desenvolvimento, de teste e de produção distintos para cada aplicação.	Equipa Informática	
	12.2	**Proteção contra código malicioso**													
	12.2.1	Controlos contra código malicioso	Sim	Sim	Implementar solução antivirus e de segurança preventiva contra malware e ataques zero-day.	X	-	X	X	-	PCs, servidores;		Instalar solução antivirus em todos os postos, servidores e equipamentos móveis.	Equipa Informática	
	12.2.1	Controlos contra código malicioso	Sim	Sim	Desenvolver ações de consciencialização dos utilizadores sobre código malicioso	X	-	X	X	-	Utilizadores;		Realizar ações públicas de consciencialização. Elaborar brochuras sobre segurança. Divulgar informação sobre segurança com regularidade. Implementar testes secretos (e.g. envio de e-mail com links suspeito) e demonstrar resultados.	Equipa Informática	
	12.3	**Salvaguarda de dados**		Sim											
	12.3.1	Salvaguarda de informação (backups)	Sim	Sim	Dispor de capacidade para efetuar a reposição de dados e de sistemas em caso de falha ou incidente de segurança .	X	X	X	X	-	Sistemas, aplicações, utilizadores;		Agendar e verificar os backups. Testar a reposição para 48h (max.)	Equipa Informática	
	12.4	**Registos de eventos e monitorização**													
	12.4.1	Registo de eventos	Não	Sim	Regular revisão de logs críticos dos sistemas.	X	-	X	X	-	Sistemas, aplicações;		Rever os logs de auditoria mensalmente.	Chefia Informática; Equipa Informática;	
	12.4.2	Proteção da informação registada	Não	Sim	Garantir a integridade dos registos nos sistemas.	X	-	X	X	-	Sistemas, aplicações, utilizadores;		Analisar registos com metadados modificados; Analisar registos com hash modificado.	Chefia Informática	
	12.4.3	Registos de administrador e de operador	Não	Sim	Conformidade com o número de atividades pelos administradores e operadores de sistemas.	X	-	X	X	-	Sistemas, aplicações, utilizadores;		Registar as atividades dos administradores e operadores de sistemas.	Chefia Informática; Equipa Informática;	
	12.4.4	Sincronização de relógio	Sim	Sim	Sincronizar o relógio dos sistemas com uma única referência horária.	X	-	X	X	-	Sistemas		Sincronizar o relógio dos sistemas com o DC.	Chefia Informática; Equipa Informática;	
	12.5	**Controlo de software em sistemas de produção**													

Anexo VIII - Declaração de Aplicabilidade

Anexo A da norma NP ISO/IEC 27001:2013			Controlo existente	Controlo a aplicar	Descrição e justificação, inclusive para as exclusões, quando aplicável	Motivos para a seleção					Recursos associados	Data implementação	Resumo da implementação (o que fazer e como fazer)	Responsável	Prazo de conclusão
						RL	OC	RN/MP	RAR	N/A					
Secção	Objetivo de controlo / Controlo														
	12.5.1	Instalação de software nos sistemas de produção	Sim	Sim	Garantir que o software instalado nos sistemas está licenciado.	X	X	X	X	-	Sistemas, aplicações;		Apenas instalar o software aprovado pela Chefia Informática; Utilizar ferramentas de inventário para análise;	Chefia Informática; Equipa Informática;	
	12.6	**Gestão de vulnerabilidades técnicas**													
	12.6.1	Gestão de vulnerabilidades técnicas	Não	Sim	Conformidade das configurações de segurança dos equipamentos com a políticas.	X	-	X	X	-	Sistemas, aplicações;		Equipamentos configurados de acordo com a políticas.	Chefia Informática; Equipa Informática;	
	12.6.1	Gestão de vulnerabilidades técnicas	Não	Sim	Avaliar se os sistemas críticos estão vulneráveis a ataques maliciosos.	X	-	X	X	-	Sistemas, aplicações;		Realizar testes de penetração ou avaliação de vulnerabilidades em sistemas críticos após cada grande *release*.	Chefia Informática; Equipa Informática;	
	12.6.1	Gestão de vulnerabilidades técnicas	Não	Sim	Avaliar o nível de vulnerabilidade dos sistemas.	X	-	X	X	-	Sistemas, aplicações;		Quantificar as vulnerabilidades não corrigidas (*unpatched*).	Chefia Informática; Equipa Informática;	
	12.6.2	Restrições sobre a instalação de software	Sim	Sim	Conformidade com a política de instalação de software.	X	-	X	X	-	Sistemas, aplicações;		Apenas a equipa informática pode instalar software.	Chefia Informática; Equipa Informática;	
	12.7	**Considerações para auditoria a sistemas de informação**													
	12.7.1	Controlos de auditoria nos sistemas de informação	Não	Sim	Avaliar o impacto da realização de auditorias nos processos de negócio .	X	X	X	X	-	Sistemas, aplicações;		Identificar os processos de negócio afetados pela realização de auditoria.	Chefia Informática; Equipa Informática;	
A.13: Segurança de comunicações	**13.1**	**Gestão de segurança da rede**													
	13.1.1	Controlos da rede	Não	Sim	Avaliar o desempenho atual da *firewall*.	-	-	X	-	-	Equipamentos de rede		Contar do n.º de regras da firewall não utilizadas e propor eliminação.	Chefia Informática; Equipa Informática;	
	13.1.2	Segurança de serviços de rede	Não	Sim	Conformidade com os serviços de rede identificados na política de segurança da rede.	-	-	X	-	-	Equipamentos de rede		Identificar serviços de rede não necessários e propor desativação.	Chefia Informática; Equipa Informática;	
	13.1.3	Segregação das redes	Não	Sim	Conformidade das VLANs com a política de segurança da rede.	-	-	X	-	-	Equipamentos de rede		Identificar VLANs, routers e desenvolver arquitetura da rede com segregação.	Chefia Informática; Equipa Informática;	
	13.2	**Transferência de informação**													
	13.2.1	Políticas e procedimentos de transferência de informação	Não	Sim	Ligações de dados encriptadas para a transferência de informação.	X	X	X	X	-	Equipamentos de rede, sistemas, serviço de rede;		VPN + IPsec para ligações a redes remotas e aplicações desktop; Certificados SSL/TLS para acesso a serviços e aplicações web;	Chefia Informática; Equipa Informática;	
	13.2.1	Políticas e procedimentos de transferência de informação	Não	Sim	Estabelecer sessões seguras (HTTPS) para aplicações web.	X	X	X	X	-	Aplicações		Utilizar certificados SSL/TLS nas aplicações web.	Chefia Informática	
	13.2.2	Acordos sobre transferência de informação	Não	Sim	Estabelecer protocolos que impõem a transferência segura da informação.	X	X	X	X	-	Equipamentos de rede, sistemas, serviço de rede;		Acordos devem contemplar prévia avaliação do risco de ligações WAN a outras entidades.	Equipa Informática	
	13.2.3	Mensagens eletrónicas	Não	Sim	Proteger a comunicação de mensagens de correio eletrónico.	X	X	X	X	-	Contas de correio eletrónico		Encriptar e assinar digitalmente as mensagens de correio eletrónico.	Equipa Informática; Utilizadores;	
	13.2.4	Acordos de confidencialidade ou de não divulgação	Não	Sim	Acordos com colaboradores, prestadores de serviços e parceiros.	X	X	X	X	-	Utilizadores;		Identificar os requisitos para acordos de confidencialidade; Acordos assinados;	Chefia Informática	
	16.1	**Gestão de incidentes de segurança da informação e melhorias**													

Anexo VIII - Declaração de Aplicabilidade

Anexo A da norma NP ISO/IEC 27001:2013			Controlo existente	Controlo a aplicar	Descrição e justificação, inclusive para as exclusões, quando aplicável	Motivos para a seleção					Recursos associados	Data implementação	Resumo da implementação (o que fazer e como fazer)	Responsável	Prazo de conclusão
						RL	OC	RN/MP	RAR	RVA					
Secção	Objetivo de controlo / Controlo														
A.16: Gestão de incidentes de segurança da informação	16.1.1	Responsabilidades e procedimentos	Sim	Sim	Definir planos de resposta (Resposta a Incidentes e Continuidade do Negócio) e planos de recuperação (Recuperação de Incidentes e Recuperação de Incidentes)	X	X	X	X	-	Sistemas, Utilizadores;		Simulação (treino) de ocorrência de incidentes;	Chefia Informática; Equipa Informática;	
	16.1.1	Responsabilidades e procedimentos	Não	Sim	Papéis atribuídos e ordem de intervenção.	X	-	X	X	-	Utilizadores;		Atribuir papel a uma pessoa; Estabelecer ordem de intervenção de acordo com o tipo de incidente;	Chefia Informática; Equipa Informática;	
	16.1.2	Reportar eventos de segurança da informação	Não	Sim	Utilizar os canais de gestão estabelecidos para reporte interno e às entidades obrigatórias por lei.	X	-	X	X	-	Utilizadores;		Preparar documentos de reporte de incidentes;	Chefia Informática; GAC;	
	16.1.3	Reportar pontos fracos de segurança da informação	Não	Sim	Pontos fracos, observados ou suspeitos, devem ser resportados por colaboradores ou prestadores de serviços.	X	-	X	X	-	Sistemas, aplicações, utilizadores;		Registo dos pontos fracos identificados; Mitigar o ponto fraco;	Chefia Informática; Equipa Informática; Utilizadores;	
	16.1.4	Avaliação e decisão sobre eventos de segurança da informação detetados	Não	Sim	Para identificar os alvos, os métodos de ataque e o potencial de impacto.	X	X	X	X	-	Sistemas, aplicações;		Analisar logs; Ativar plano de resposta a incidentes;	Chefia Informática; Equipa Informática;	
	16.1.4	Avaliação e decisão sobre eventos de segurança da informação detetados	Não	Sim	Categorizar os incidentes para consistência com os planos de resposta.	X	X	X	X	-	Sistemas, aplicações;		Elaborar lista de categorias de incidentes; Mapeamento entre categorias, incidentes e planos de resposta;	Chefia Informática; Equipa Informática;	
	16.1.5	Resposta a incidentes de segurança da informação	Não	Sim	Estabelecer plano de resposta e recuperação de incidentes	X	X	X	X	-	Sistemas, Utilizadores;		Executar o plano de resposta a incidente durante ou após o evento.	Chefia Informática; Equipa Informática;	
	16.1.5	Resposta a incidentes de segurança da informação	Não	Sim	Investigar as notificações de segurança dos sistemas.	X	X	X	X	-	Utilizadores;		Identificar origem e sistema alvo de ataque, serviços afetados, portas utilizadas; Analisar logs.	Chefia Informática; Equipa Informática;	
	16.1.6	Aprender com os incidentes de segurança da informação	Sim	Sim	Comunicação em rede entre entidades.	X	X	X	X	-	Sistemas, Utilizadores;		Partilhar informação sobre a eficácia de tecnologias de informação. Criar "knowledgebase".	Chefia Informática; Equipa Informática;	
	16.1.6	Aprender com os incidentes de segurança da informação	Não	Sim	Melhoria continua dos processos de deteção de incidentes.	X	X	X	X	-	Sistemas, Utilizadores;		Medir a capacidade dos processos em vigor com Modelo de Capacidade do COBIT 5.	Chefia Informática; Equipa Informática;	
	16.1.6	Aprender com os incidentes de segurança da informação	Não	Sim	Melhoria continua dos planos de resposta.	X	X	X	X	-	Sistemas, Utilizadores;		Incluir lições aprendidas nos planos de resposta.	Chefia Informática; Equipa Informática;	
	16.1.7	Recolha de evidências	Sim	Sim	Recolha de logs	X	X	X	X	-	Sistemas, Utilizadores;		Isolar sistema/equipamento alvo de incidente; Efetuar imagem do sistema; Recolher logs;	Chefia Informática; Equipa Informática;	

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.5 - Políticas de segurança da informação

A.5.1 - Diretrizes da gestão para a segurança da informação

Controlo	A.5.1.1 – Políticas para a segurança da informação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se as políticas de segurança da informação necessárias são estabelecidas.
Medida	Percentagem de políticas estabelecidas.
Fórmula/Pontuação	(N.º de políticas de segurança de informação estabelecidas no último ano/Total de políticas de segurança da informação a estabelecer) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	Verde
Evidência de implementação	Documento que estabelece a política.
Frequência	Recolha de medições: anual Relatório: um para cada medição
Partes responsáveis	CA: responsável pela informação e pelo desenvolvimento, revisão e avaliação das políticas Chefia Informática: responsável pela medição
Fonte de dados	Plano de definição de políticas
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.5 - Políticas de segurança da informação

A.5.1 - Diretrizes da gestão para a segurança da informação

Controlo	A.5.1.2 - Revisão das políticas para a segurança da informação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se as políticas de segurança da informação são revistas em intervalos planeados ou se ocorrem mudanças significativas.
Medida	Percentagem de políticas revistas.
Fórmula/Pontuação	(N.º de políticas de segurança de informação revistas no último ano/Total de políticas de segurança da informação em vigor) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	Verde
Evidência de implementação	Histórico do documento mencionando as revisões efetuadas ou documento indicando a data da última revisão.
Frequência	Recolha de medições: anual ou após alterações significativas Relatório: um para cada medição
Partes responsáveis	CA: responsável pela informação e pelo desenvolvimento, revisão e avaliação das políticas Chefia Informática: responsável pela medição
Fonte de dados	Plano de revisão de políticas, histórico de revisão da política
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.1 - Procedimentos e responsabilidades operacionais

Controlo	A.12.1.1 – Procedimentos de operação documentados
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se os procedimentos de operação são documentados e disponibilizados aos utilizadores.
Medida	Número de procedimentos documentados e disponibilizados.
Fórmula/Pontuação	Contagem do n.º de procedimentos documentados e disponibilizados
Alvo	Verde
Evidência de implementação	Documento com os procedimentos de operação dos recursos de processamento de informação.
Frequência	Recolha de medições: anual ou após alterações significativas Relatório: um para cada medição
Partes responsáveis	Chefia Informática: responsável pela aprovação dos procedimentos e pela medição do controlo Equipa informática: responsável pela definição dos procedimentos
Fonte de dados	Lista de operações realizadas
Formato de reporte	Relatório

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.1 - Procedimentos e responsabilidades operacionais

Controlo	A.12.1.2 – Gestão de alterações
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se as boas práticas de gestão de alterações são cumpridas.
Medida	Percentagem de novas aplicações desenvolvidas em cumprimento com as boas práticas de gestão de alterações.
Fórmula/Pontuação	(N.º de novas aplicações desenvolvidas em cumprimento com as boas práticas de gestão de alterações/Total de novas aplicações desenvolvidas) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Registo de alterações Registo de versões
Frequência	Recolha de medições: semestral Relatório: semestral, a enviar à Chefia Informática
Partes responsáveis	Chefia Informática: responsável pela definição das boas práticas de gestão de alterações e pela medição do controlo Equipa informática: responsável pela aplicação das boas práticas de gestão de alterações
Fonte de dados	Sistema gestor de repositório de software
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.1 - Procedimentos e responsabilidades operacionais

Controlo	A.12.1.3 – Gestão da capacidade
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se a capacidade em disco dos sistemas é ajustada aos requisitos para o seu bom funcionamento.
Medida	Percentagem de capacidade disponível em cada sistema.
Fórmula/Pontuação	(Capacidade disponível em cada sistema/Total de capacidade em cada sistema) *100 Vermelho < 40%; Laranja <= 60%; Verde > 60%
Alvo	>= 40%
Evidência de implementação	Relatório de desempenho sobre utilização do espaço em disco
Frequência	Recolha de medições: semestral Relatório: semestral, a enviar à Chefia Informática
Partes responsáveis	Chefia Informática: responsável pela definição da capacidade adequada a cada sistema e pela medição do controlo Equipa informática: responsável pela monitorização da utilização dos recursos dos sistemas
Fonte de dados	Monitor de recursos do sistema
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.1 - Procedimentos e responsabilidades operacionais

Controlo	A.12.1.4 – Separação entre ambientes de desenvolvimento, teste e de produção
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a separação entre os ambientes de desenvolvimento, de teste e de produção
Medida	Percentagem de ambientes, por aplicação, separados entre si.
Fórmula/Pontuação	(Número de ambientes por aplicação separados entre si/Total de ambientes por aplicação separados entre si) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	Cada aplicação deve ter um ambiente de desenvolvimento, um ambiente de teste e um ambiente de produção, separados entre si.
Evidência de implementação	Documento com identificação de cada ambiente (equipamento, sistema, versão da aplicação, utilizadores, permissões, ...) para as respetivas aplicações
Frequência	Recolha de medições: semestral Relatório: semestral, a enviar à Chefia Informática
Partes responsáveis	Chefia Informática: responsável pela definição dos ambientes e pela medição do controlo Equipa informática: responsável pela utilização correta dos ambientes
Fonte de dados	Relatório de atividades de desenvolvimento realizadas, de testes definidos e realizados e *logs* dos sistemas em ambiente de produção
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.2 – Proteção contra código malicioso

Controlo	A.12.2.1 – Controlos contra código malicioso (1 de 2)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a eficácia do sistema de proteção contra ataques maliciosos
Medida	Número de incidentes
Fórmula/Pontuação	Contagem do número de incidentes de segurança não bloqueados
Alvo	Zero
Evidência de implementação	Monitorização das atividades de antivírus e segurança nos sistemas
Frequência	Recolha de medições: diária (no sistema) Análise: semanal para os incidentes Relatório: semanal para os incidentes, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pela gestão do sistema de proteção e pela medição do controlo Equipa informática: responsável pela monitorização, prevenção e recuperação dos incidentes
Fonte de dados	Ferramentas de monitorização Consola do sistema de proteção contra ataques maliciosos
Formato de reporte	Relatório

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.2 – Proteção contra código malicioso

Controlo	A.12.2.1 – Controlos contra código malicioso (2 de 2)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a participação dos utilizadores em ações de consciencialização
Medida	Percentagem de utilizadores que participaram em ações de consciencialização
Fórmula/Pontuação	(Número de utilizadores que participaram em ações de consciencialização/Total de utilizadores da empresa) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Relatório de ações de consciencialização realizadas
Frequência	Recolha de medições: semestral Análise: anual Relatório: anual, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pelo planeamento das ações de consciencialização e pela medição do controlo Equipa informática: responsável ministrar as ações de consciencialização
Fonte de dados	Relatório de ações de consciencialização realizadas
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.3 – Salvaguarda de dados

Controlo	A.12.3.1 – Salvaguarda de informação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a reposição de dados e de sistemas em caso de falha ou incidente de segurança
Medida	Percentagem dos dados e sistemas que necessitando ser repostos, são repostos em 48h (max.)
Fórmula/Pontuação	(Número de reposições até 48h/ Total de reposições) *100
Alvo	100%
Evidência de implementação	Relatório dos *backups* e testes de reposição realizados
Frequência	Recolha de medições: diária Análise: semanal Relatório: semanal, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pelo planeamento dos *backups* em conformidade com a política de backup e pela medição do controlo Equipa informática: responsável pela monitorização dos backups, testes de integridade e reposição dos dados e sistemas
Fonte de dados	*Logs* do sistema de *backup*, indicando o tempo necessário para executar cada reposição.
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.4 – Registos de eventos e monitorização

Controlo	A.12.4.1 – Registos de eventos
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o estado de conformidade com a regular revisão de *logs* críticos dos sistemas
Medida	Número de *logs* de com erros
Fórmula/Pontuação	(Número de *logs* com erros revistos /Total de *logs* com erros) * 100 Vermelho > 80%; Laranja >= 40%; Verde < 40%
Alvo	0%
Evidência de implementação	Soma do número total de *logs* que constam na lista de *logs* revistos
Frequência	Recolha de medições: mensal Análise: mensal Relatório: trimestral, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pela análise dos *logs* críticos, pela instrução à equipa informática das ações para resolução dos problemas identificados e pela medição do controlo Equipa informática: responsável pela recolha dos *logs* críticos e resolução dos problemas identificados
Fonte de dados	Sistema e ficheiros de *log*
Formato de reporte	Relatório

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.4 – Registos de eventos e monitorização

Controlo	A.12.4.2 – Proteção da informação registada
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o estado de integridade dos registos nos sistemas
Medida	Sem encriptação: percentagem de registos com metadados modificados Com encriptação: percentagem de registos com *hash* diferente
Fórmula/Pontuação	Contagem do n.º de registos com atributos modificados Contagem do n.º de registos com hash modificado
Alvo	0
Evidência de implementação	Relatório sobre integridade dos registos nos sistemas
Frequência	Recolha de medições: mensal Análise: mensal Relatório: trimestral, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pela implementação dos mecanismos de encriptação e pela medição do controlo
Fonte de dados	Sistema, ficheiros e *logs*
Formato de reporte	Relatório

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.4 – Registos de eventos e monitorização

Controlo	A.12.4.3 – Registos de administrador e de operador
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar as atividades realizadas pelos administradores e operadores de sistemas
Medida	Percentagem de atividades dos administradores e operadores de sistemas por período de tempo
Fórmula/Pontuação	(N.º de registos de atividades no período definido/Total de atividades) *100
Alvo	Resultado abaixo de 20% deve ser analisado por motivos de baixo desempenho Resultado 20% acima deve ser analisado por motivos de clarificação das atividades realizadas
Evidência de implementação	Soma do número total de *logs* que constam na lista de *logs* revistos
Frequência	Recolha de medições: mensal Análise: mensal Relatório: trimestral
Partes responsáveis	Chefia Informática: responsável pelo controlo e revisão das atividades dos administradores e operadores de sistemas e pela medição do controlo Equipa informática: responsável pelo registo de atividades realizadas
Fonte de dados	Sistema, ficheiros de log, relatórios
Formato de reporte	Relatório

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.4 – Registos de eventos e monitorização

Controlo	A.12.4.4 – Sincronização de relógio
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o estado de sincronização do relógio dos sistemas com uma única referência horária
Medida	Percentagem de relógios sincronizados com uma única referência horária
Fórmula/Pontuação	(N.º de relógios sincronizados/Total de relógios) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Hora igual em todos os sistemas
Frequência	Recolha de medições: semanal Análise: semanal Relatório: mensal, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pela escolha da referência horária a utilizar e pela medição do controlo Equipa informática: responsável pela monitorização do relógio dos sistemas e reporte de falhas na escrita por motivos de tempo adiantado.
Fonte de dados	Sistema
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.5 – Controlo de *software* em sistemas de produção

Controlo	A.12.5.1 – Instalação de *software* nos sistemas de produção
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o estado do licenciamento do *software* instalado nos sistemas
Medida	Percentagem de *software* licenciado
Fórmula/Pontuação	(N.º de aplicações licenciadas/Total de aplicações instaladas) *100
Alvo	100%
Evidência de implementação	Registos de licenciamento
Frequência	Recolha de medições: mensal Análise: mensal Relatório: mensal, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pela definição do *software* autorizado e pela medição do controlo Equipa informática: responsável pela instalação de *software*.
Fonte de dados	Ferramentas de inventário de *software* e de controlo de licenças
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.6 – Gestão de vulnerabilidades técnicas

Controlo	A.12.6.1 – Gestão de vulnerabilidades técnicas (1 de 3)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o estado de conformidade das configurações de segurança dos equipamentos com as políticas
Medida	Percentagem de equipamentos configurados de acordo com as políticas
Fórmula/Pontuação	(N.º de equipamentos configurados corretamente/Total de equipamentos) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Inventário de equipamentos, *software* e configurações
Frequência	Recolha de medições: cada 3 dias Análise: cada 3 dias Relatório: imediato, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável análise de vulnerabilidades detetadas e pela medição do controlo Equipa informática: responsável pela monitorização e deteção de vulnerabilidades
Fonte de dados	Ferramentas de inventário de *software*
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.6 – Gestão de vulnerabilidades técnicas

Controlo	A.12.6.1 – Gestão de vulnerabilidades técnicas (2 de 3)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se os sistemas críticos estão vulneráveis a ataques maliciosos
Medida	Percentagem de sistemas críticos com avaliação de vulnerabilidades realizada desde a última grande *release*.
Fórmula/Pontuação	(N.º de sistemas críticos com avaliação de vulnerabilidades realizada desde a última grande *release*/Total de sistemas críticos) *100 Verde = 100%; Laranja >= 75%; Vermelho < 75%
Alvo	Verde
Evidência de implementação	Relatórios de avaliações de vulnerabilidades executadas nos sistemas críticos
Frequência	Recolha de medições: anual Relatório: um para cada medição, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pela definição dos testes de penetração, avaliação de vulnerabilidades e pela medição do controlo Equipa informática: responsável pela execução dos testes de penetração
Fonte de dados	Inventário de bens, relatórios de testes de penetração
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.6 – Gestão de vulnerabilidades técnicas

Controlo	A.12.6.1 – Gestão de vulnerabilidades técnicas (3 de 3)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o nível de vulnerabilidade dos sistemas críticos
Medida	Quantificação das vulnerabilidades não corrigidas (*unpatched*)
Fórmula/Pontuação	Gravidade da vulnerabilidade[9] * Total de sistemas críticos afetados
Alvo	A definir de acordo com o nível de risco aceite pela empresa
Evidência de implementação	Análise das atividades de avaliação de vulnerabilidades
Frequência	Recolha de medições: trimestral Relatório: um para cada medição, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pela avaliação de vulnerabilidades e pela medição do controlo Equipa informática e utilizadores: responsável pela deteção de vulnerabilidades
Fonte de dados	Relatórios e ferramentas de avaliação de vulnerabilidades
Formato de reporte	Valores de pontuação agregados por tipo de ativo.

[9] Calculada através do *Common Vulnerability Scoring System Calculator (Version 3)*

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.6 – Gestão de vulnerabilidades técnicas

Controlo	A.12.6.2 – Restrições sobre a instalação de *software*
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o estado de conformidade com a política de instalação de *software*
Medida	Percentagem de *software* instalado pelos utilizadores
Fórmula/Pontuação	(N.º de aplicações instaladas pelos utilizadores/Total de instalações) *100 Verde = 0%; Laranja <= 80%; Vermelho > 80%
Alvo	0 %
Evidência de implementação	Relatórios de inventário de *software* (*scan* em tempo-real)
Frequência	Recolha de medições: trimestral Relatório: um para cada medição, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pelo cumprimento da política de instalação de *software* e pela medição do controlo Equipa informática: responsável pela deteção de instalação indevida de *software* Utilizadores: responsáveis por instalações indevidas
Fonte de dados	Relatórios e ferramentas de inventário
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.12 – Segurança de operações

A.12.7 – Considerações para auditorias a sistemas de informação

Controlo	A.12.7.1 – Controlos de auditoria nos sistemas de informação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o impacto da realização de auditorias nas atividades dos serviços
Medida	Tempo de inatividade dos serviços devido a realização de auditoria
Fórmula/Pontuação	Contagem do tempo de inatividade dos serviços afetados pela realização de auditoria
Alvo	0 minutos ou tão baixo quanto possível
Evidência de implementação	Relatório do impacto verificado
Frequência	Recolha de medições: anual Relatório: um para cada medição, a enviar ao CA;
Partes responsáveis	Chefia Informática: responsável pelo estudo de impacto, pelo planeamento da auditoria de forma a minimizar as interrupções nos processos de negócio e pela medição do controlo
Fonte de dados	Sistemas alvo de auditoria, lista de processos
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.1 – Controlos da rede (1 de 6)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o desempenho atual da *firewall*
Medida	Regras sem utilização na *firewall*
Fórmula/Pontuação	Contagem do n.º de regras da *firewall* não utilizadas
Alvo	0
Evidência de implementação	Registos dos contadores de utilização (Hits) em cada regra da *firewall*
Frequência	Recolha de medições: semestral
Partes responsáveis	Chefia Informática: responsável pela gestão dos ativos de rede e pela medição do controlo
Fonte de dados	Consola de gestão da *firewall*
Formato de reporte	Lista de regras da *firewall* não utilizadas para identificar como “a rever” e possível eliminação.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.1 – Controlos da rede (2 de 6)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a exposição ao risco da infraestrutura face à localização dos servidores *Web*
Medida	Servidores *Web* fora da DMZ com dupla *firewall*
Fórmula/Pontuação	Contagem do n.º de servidores *Web* fora da DMZ com dupla *firewall*/Total de servidores *Web*
Alvo	0
Evidência de implementação	Configurações de rede
Frequência	Recolha de medições: anual
Partes responsáveis	Chefia Informática: responsável pela gestão dos ativos de rede e pela medição do controlo
Fonte de dados	Sistemas
Formato de reporte	Relatório e diagrama da rede

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.1 – Controlos da rede (3 de 6)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a utilização dada aos *switches* atendendo às configurações de segurança disponíveis no *software*
Medida	Percentagem de *switches* com *software* de gestão efetivamente utilizado
Fórmula/Pontuação	(N.º de *switches* com software de gestão efetivamente utilizado/Total de *switches*) *100
Alvo	100%
Evidência de implementação	Configurações implementadas
Frequência	Recolha de medições: anual
Partes responsáveis	Chefia Informática: responsável pela gestão dos ativos de rede e pela medição do controlo
Fonte de dados	*Switches*
Formato de reporte	Relatório de configurações implementadas

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.1 – Controlos da rede (4 de 6)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a eficácia de bloqueio do sistema de deteção e prevenção de intrusões (IDS/IPS)
Medida	Percentagem de tentativas de intrusão bloqueadas
Fórmula/Pontuação	(N.º de tentativas de intrusão bloqueadas/Total de tentativas de intrusão) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Configurações implementadas
Frequência	Recolha de medições: diária
Partes responsáveis	Chefia Informática: responsável pela gestão dos ativos de rede e pela medição do controlo
Fonte de dados	Registos no IDS/IPS, *routers, firewall, switches*
Formato de reporte	Relatório de resultados diários sobre tentativas de intrusão

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.1 – Controlos da rede (5 de 6)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o estado de atualização do *firmware* dos equipamentos de rede
Medida	Percentagem de equipamentos com *firmware* atualizado
Fórmula/Pontuação	(N.º de equipamentos de rede com *firmware* atualizado /Total equipamentos de rede) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Verificação da versão atual
Frequência	Recolha de medições: semanal
Partes responsáveis	Chefia Informática: responsável pela gestão dos ativos de rede e pela medição do controlo
Fonte de dados	Registos no IDS/IPS, *routers, firewall, switches*
Formato de reporte	Relatório de resultados diários sobre tentativas de intrusão

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.1 – Controlos da rede (6 de 6)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a ocorrência de *spoofing*
Medida	Percentagem de registos estáticos de IP e MAC *Address* nos *switches* e *routers*
Fórmula/Pontuação	(N.º de IPs e MAC *Addresses* registados nas tabelas dos switches e routers/Total equipamentos) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Verificação da versão atual
Frequência	Recolha de medições: semanal
Partes responsáveis	Chefia Informática: responsável pela gestão dos ativos de rede e pela medição do controlo
Fonte de dados	*Switches, routers*, Sistema IDS/IPS
Formato de reporte	Relatório de resultados diários sobre tentativas de intrusão

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.2 – Segurança de serviços de rede (1 de 5)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o estado de conformidade com os serviços de rede identificados na política de segurança da rede
Medida	Percentagem de serviços de rede não necessários
Fórmula/Pontuação	(N.º de serviços de rede não necessários/Total de serviços de rede) *100 Verde < 20%; Laranja <= 80%; Vermelho > 80%
Alvo	0%
Evidência de implementação	Inventário de serviços
Frequência	Recolha de medições: semestral
Partes responsáveis	Chefia Informática: responsável pela gestão dos ativos de rede e pela medição do controlo
Fonte de dados	Sistemas, consola de gestão da *firewall*, de *routers*, *switches,* de *access points*
Formato de reporte	Relatório de serviços ativados, mas não necessários, para identificar como “a rever” e possível desativação.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.2 – Segurança de serviços de rede (2 de 5)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o *broadcast* de SSID nos *Access Points*
Medida	Percentagem de *APs* com SSID oculto
Fórmula/Pontuação	(N.º de *APs* com SSID oculto/Total de *APs*) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Configuração dos *APs*
Frequência	Recolha de medições: anual
Partes responsáveis	Equipa Informática: responsável pela configuração dos *APs*
Fonte de dados	*Access Points*
Formato de reporte	Relatório de configuração

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.2 – Segurança de serviços de rede (3 de 5)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a utilização do protocolo WPA2 802.11i (*Robust Security Network*) nos *Access Points*
Medida	Percentagem de *APs* configurados com WPA2 802.11i
Fórmula/Pontuação	(N.º de *APs* configurados com WPA2 802.11i /Total de *APs*) *100
Alvo	100%
Evidência de implementação	Configuração dos *APs*
Frequência	Recolha de medições: anual
Partes responsáveis	Equipa Informática: responsável pela configuração dos *APs*
Fonte de dados	*Access Points*
Formato de reporte	Relatório de configuração

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.2 – Segurança de serviços de rede (4 de 5)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o *auto-discovery* de dispositivos Bluetooth
Medida	Percentagem de dispositivos *Bluetooth* com *auto-discovery* ativado
Fórmula/Pontuação	(N.º de dispositivos *Bluetooth* com *auto-discovery* ativado /Total de dispositivos *Bluetooth*) *100 Verde < 20%; Laranja <= 80%; Vermelho > 80%
Alvo	0%
Evidência de implementação	Configuração dos dispositivos Bluetooth
Frequência	Recolha de medições: semestral
Partes responsáveis	Equipa Informática: responsável pela configuração dos dispositivos Bluetooth
Fonte de dados	Dispositivos Bluetooth
Formato de reporte	Relatório de configuração

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.2 – Segurança de serviços de rede (5 de 5)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a qualidade das respostas a pesquisas DNS
Medida	Percentagem de zonas DNS protegidas com DNSSEC
Fórmula/Pontuação	(N.º de zonas DNS protegidas com DNSSEC/Total de zonas DNS protegidas com DNSSEC) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Configuração das zonas de pesquisa
Frequência	Recolha de medições: semestral
Partes responsáveis	Chefia Informática: responsável pela gestão dos ativos de rede e pela medição do controlo
Fonte de dados	Sistemas, serviço DNS
Formato de reporte	Relatório

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.3 – Segregação das redes (1 de 2)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o estado de conformidade das VLANs com a política de segurança da rede
Medida	Percentagem de acessos indevidos a VLANs
Fórmula/Pontuação	(N.º de acessos indevidos a VLANs/Total de acessos a VLANs) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	0%
Evidência de implementação	Integridade da rede Relatório de testes
Frequência	Recolha de medições: semestral Relatório: um para cada medição, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pelo planeamento das VLANs e pela medição do controlo Equipa Informática: responsável pela realização de testes de acesso às VLANs
Fonte de dados	Sistemas, consola de gestão de *routers*, de *switches,* de *access points*
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.1 – Gestão de segurança da rede

Controlo	A.13.1.3 – Segregação das redes (2 de 2)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a eficácia do isolamento de portas nas VLANs
Medida	Pedidos de acesso entre sistemas residentes no mesmo *hypervisor*
Fórmula/Pontuação	Contagem do n.º de pedidos de acesso entre sistemas residentes no mesmo *hypervisor*
Alvo	0 (excluindo as ligações aos servidores de domínio)
Evidência de implementação	Configuração de *port isolation* no *switch*
Frequência	Recolha de medições: semestral
Partes responsáveis	Chefia Informática: responsável pelo planeamento das VLANs e pela medição do controlo Equipa Informática: responsável pela realização de testes de acesso às VLANs
Fonte de dados	Hypervisor, sistemas virtualizados, *switches*
Formato de reporte	Relatório

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.2 – Transferência de informação

Controlo	A.13.2.1 – Políticas e procedimentos de transferência de informação (1 de 2)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o mapeamento das comunicações organizacionais existentes em conformidade com a política de segurança da rede
Medida	Percentagem de ligações de dados não encriptadas
Fórmula/Pontuação	(N.º de ligações de dados não encriptadas/Total de ligações) *100 Verde < 20%; Laranja <= 80%; Vermelho > 80%
Alvo	0%
Evidência de implementação	SSH para upload de ficheiros para a cloud VPN + IPsec para ligações a redes remotas e aplicações desktop Certificados SSL/TLS para acesso a serviços e aplicações *Web* Certificados X.509 para autenticação
Frequência	Recolha de medições: anual
Partes responsáveis	Chefia Informática: responsável pela implementação dos mecanismos de segurança e pela medição do controlo
Fonte de dados	Sistemas, aplicações, *router*, *firewall*
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.2 – Transferência de informação

Controlo	**A.13.2.1 – Políticas e procedimentos de transferência de informação (2 de 2)**
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a utilização de sessões seguras (HTTPS) em conformidade com a política de segurança da rede
Medida	Percentagem de aplicações *Web* com estabelecimento de sessão segura
Fórmula/Pontuação	(N.º de aplicações *Web* com estabelecimento de sessão segura /Total de aplicações *Web*) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Certificados SSL/TLS
Frequência	Recolha de medições: anual
Partes responsáveis	Chefia Informática: responsável pela implementação dos mecanismos de segurança e pela medição do controlo
Fonte de dados	Sistemas, aplicações, *router*, *firewall*
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.2 – Transferência de informação

Controlo	A.13.2.2 – Acordos sobre transferência de informação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar os protocolos de transferência de informação para entidades externas
Medida	Percentagem de protocolos que impõem a transferência segura da informação
Fórmula/Pontuação	(N.º de protocolos que impõem a transferência segura da informação /Total de protocolos) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Documento assinado entre as partes que estabelece a utilização dos meios de comunicação seguros adequados à transferência da informação
Frequência	Recolha de medições: anual Relatório: um para cada medição, a enviar ao CA
Partes responsáveis	CA: responsável pelos protocolos Chefia Informática: responsável pela implementação dos mecanismos de segurança e pela medição do controlo
Fonte de dados	Protocolos
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.2 – Transferência de informação

Controlo	A.13.2.3 – Mensagens eletrónicas
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a proteção da informação contida em e-mails
Medida	N.º de certificados de encriptação/autenticação por aplicação com funcionalidades de e-mail
Fórmula/Pontuação	Contagem do n.º certificados por aplicação com funcionalidades de e-mail
Alvo	Todas as mensagens eletrónicas são encriptadas
Evidência de implementação	Certificados instalados
Frequência	Recolha de medições: anual Relatório: um para cada medição, a enviar à Chefia Informática;
Partes responsáveis	Chefia Informática: responsável pela gestão dos certificados e pela medição do controlo Equipa Informática: responsável pela instalação dos certificados Utilizadores: responsáveis por encriptar/assinar digitalmente as mensagens eletrónicas
Fonte de dados	Aplicações com funcionalidades de e-mail
Formato de reporte	Relatório de instalação dos certificados

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.13 – Segurança de comunicações

A.13.2 – Transferência de informação

Controlo	A.13.2.4 – Acordos de confidencialidade e de não divulgação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se os acordos de confidencialidade ou de não divulgação são cumpridos.
Medida	Percentagem de acordos de confidencialidade e de não divulgação que são cumpridos.
Fórmula/Pontuação	(N.º de acordos de confidencialidade ou de não divulgação são cumpridos/Total de acordos de confidencialidade ou de não divulgação) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Documento com os requisitos estabelecidos para os acordos
Frequência	Recolha de medições: anual Relatório: anual, a enviar ao CA
Partes responsáveis	Chefia Informática: responsável pela definição dos requisitos a constar nos acordos e pela medição do controlo
Fonte de dados	Documentos de acordos de confidencialidade estabelecidos
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	A.16.1.1 – Responsabilidades e procedimentos (1 de 2)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a conformidade dos planos de resposta e recuperação de incidentes com a política de gestão de incidentes de segurança da informação
Medida	Percentagem de planos de resposta e de recuperação em conformidade
Fórmula/Pontuação	(N.º de planos de resposta e recuperação em conformidade /Total de planos de resposta e recuperação) *100
Alvo	100%
Evidência de implementação	Documentos com procedimentos legais para resposta a incidentes Documentos com procedimentos técnicos para recuperação Simulação (treino) de ocorrência de incidentes Resultados dos treinos realizados
Frequência	Recolha de medições: semestral Relatório: um para cada medição, a enviar ao CA;
Partes responsáveis	CA: responsável pela aprovação dos planos de resposta e recuperação Chefia Informática: responsável pela gestão da resposta e recuperação de incidentes e pela medição do controlo Equipa Informática: responsável pela aplicação dos procedimentos de recuperação de incidentes
Fonte de dados	Planos de resposta e recuperação, legislação, sistemas
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	A.16.1.1 – Responsabilidades e procedimentos (2 de 2)
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a conformidade dos papéis com a política de gestão de incidentes de segurança da informação
Medida	Papéis atribuídos
Fórmula/Pontuação	Cada papel atribuído a uma pessoa
Alvo	Desempenho adequado em caso de incidente
Evidência de implementação	Comunicação escrita das responsabilidades na resposta a incidentes Receção validada pelos intervenientes Simulação (treino) de ocorrência de incidentes Resultados dos treinos realizados
Frequência	Recolha de medições: anual Relatório: um para cada medição, a enviar ao CA;
Partes responsáveis	Chefia Informática: responsável pelo planeamento da resposta e recuperação de incidentes e pela medição do controlo Equipa Informática: responsável pela aplicação dos procedimentos de recuperação de incidentes
Fonte de dados	Planos de resposta e recuperação, legislação, sistemas
Formato de reporte	Relatório

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	A.16.1.2 – Reportar eventos de segurança da informação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o reporte de incidentes de segurança
Medida	Número de incidentes de segurança reportados num ano
Fórmula/Pontuação	(N.º de incidentes de segurança reportados num ano /Total de incidentes de segurança num ano) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Documentos de reporte enviados
Frequência	Recolha de medições: anual
Partes responsáveis	Chefia Informática: responsável pelo registo de incidentes e pela medição do controlo
Fonte de dados	Registo anual de incidentes
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	A.16.1.3 – Reportar pontos fracos de segurança da informação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar o reporte de pontos fracos de segurança da informação, observados ou suspeitos, por colaboradores ou prestadores de serviços
Medida	Percentagem de reportes de pontos fracos
Fórmula/Pontuação	(N.º de reportes de pontos fracos realizados/Total de pontos fracos confirmados) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	100%
Evidência de implementação	Documento com instruções de reporte de pontos fracos de segurança
Frequência	Recolha de medições: diária Relatório: diário, a enviar à Chefia Informática
Partes responsáveis	Chefia Informática: responsável por instruir o reporte e pela medição do controlo Equipa Informática: responsável por receber os reportes Colaboradores e prestadores de serviços: responsáveis por reportar à Equipa Informática os pontos fracos observados ou suspeitos
Fonte de dados	Instalações físicas, sistemas, acessos, equipamentos, *software*
Formato de reporte	E-mail Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	**A.16.1.4 – Avaliação e decisão sobre eventos de segurança da informação** **(1 de 2)**
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliação dos eventos de segurança de informação detetados para identificação dos alvos, dos métodos de ataque e potencial impacto
Medida	Percentagem de eventos detetados
Fórmula/Pontuação	(N.º de avaliações realizadas a eventos detetados /Total de eventos detetados) *100
Alvo	100%
Evidência de implementação	Relatório de avaliações
Frequência	Recolha de medições: semanal Relatório: um para cada medição, a enviar ao CA;
Partes responsáveis	Chefia Informática: responsável pela avaliação dos eventos de segurança de informação detetados e pela medição do controlo Equipa Informática: recolha de informação sobre eventos de segurança da informação detetados
Fonte de dados	Lista de eventos de segurança da informação
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	**A.16.1.4 – Avaliação e decisão sobre eventos de segurança da informação** **(2 de 2)**
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar a categorização dos incidentes para consistência com os planos de resposta
Medida	Percentagem de incidentes categorizados
Fórmula/Pontuação	(N.º de incidentes categorizados /Total de incidentes) *100
Alvo	100%
Evidência de implementação	Lista de categorias de incidentes Mapeamento entre categorias, incidentes e planos de resposta Relatório de avaliações efetuadas
Frequência	Recolha de medições: semestral Relatório: um para cada medição
Partes responsáveis	Chefia Informática: responsável pela avaliação da categorização dos incidentes Equipa Informática: recolha de informação sobre incidentes
Fonte de dados	Lista de categorias de incidentes Lista de incidentes de segurança da informação Planos de resposta
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	A.16.1.5 – Resposta a incidentes de segurança da informação
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se o plano de resposta é executado durante ou após um evento (conforme estabelecido na política de gestão de incidentes de segurança da informação)
Medida	Percentagem de execução do plano de resposta num evento
Fórmula/Pontuação	(N.º de vezes que o plano de resposta foi executado/Total de eventos) *100
Alvo	100% (ação imediata)
Evidência de implementação	Relatório do impacto verificado
Frequência	Recolha de medições: anual Relatório: um para cada medição, a enviar ao CA;
Partes responsáveis	Chefia Informática: responsável pela gestão da resposta e recuperação de incidentes e pela medição do controlo Equipa Informática: responsável pela aplicação dos procedimentos de resposta e recuperação de incidentes
Fonte de dados	Planos de resposta
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	**A.16.1.6 – Aprender com os incidentes de segurança da informação (1 de 3)**
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se a eficácia das tecnologias de proteção é partilhada de forma a reduzir a probabilidade ou o impacto de futuros incidentes
Medida	Percentagem de incidentes após início de partilha de informações
Fórmula/Pontuação	(N.º de incidentes após início de partilha de informações /Total de incidentes) *100
Alvo	0% ou tão baixo quanto possível
Evidência de implementação	Relatórios de incidentes *versus* tecnologias de proteção aplicadas
Frequência	Recolha de medições: semestral Relatório: um para cada medição, a enviar ao CA;
Partes responsáveis	Chefia Informática: responsável pela decisão das tecnologias a implementar e pela medição do controlo Equipa Informática: responsável pela implementação das tecnologias de segurança
Fonte de dados	Sistemas de deteção de incidentes de segurança
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	**A.16.1.6 – Aprender com os incidentes de segurança da informação (2 de 3)**
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se os processos de deteção são continuamente melhorados
Medida	Percentagem de processos de deteção melhorados
Fórmula/Pontuação	(N.º de processos de deteção melhorados/Total de processos de deteção implementados) *100 Verde > 80%; Laranja >= 40%; Vermelho < 40%
Alvo	Verde
Evidência de implementação	Documento com definição dos processos de deteção estabelecidos Evolução das versões dos processos
Frequência	Recolha de medições: semestral Relatório: um para cada medição, a enviar ao CA;
Partes responsáveis	Chefia Informática: responsável pela decisão das tecnologias a implementar e pela medição do controlo Equipa Informática: responsável pela implementação das tecnologias de segurança
Fonte de dados	Sistemas, relatórios
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	**A.16.1.6 – Aprender com os incidentes de segurança da informação (3 de3)**
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se os planos de resposta incluem as lições aprendidas
Medida	Planos de resposta melhorados
Fórmula/Pontuação	Contagem do n.º de planos de resposta melhorados
Alvo	N.º de planos de resposta melhorados >= N.º de incidentes
Evidência de implementação	Documento com definição dos processos de deteção estabelecidos Evolução das versões dos processos
Frequência	Recolha de medições: semestral Relatório: um para cada medição, a enviar ao CA;
Partes responsáveis	Chefia Informática: responsável pela gestão da resposta e recuperação de incidentes e pela medição do controlo Equipa Informática: responsável pela aplicação dos procedimentos de resposta e recuperação de incidentes
Fonte de dados	Planos de resposta
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo IX - Programa de Implementação do SGSI - Monitorização e medição da eficácia dos controlos

Secção A.16 – Gestão de incidentes de segurança

A.16.1 – Gestão de incidentes de segurança da informação e melhorias

Controlo	A.16.1.7 – Recolha de evidências
ID da medição	Numeração a definir pela IHM
Necessidade de informação	Avaliar se é realizada atividade forense após a ocorrência de incidentes
Medida	Atividade forense realizada
Fórmula/Pontuação	Contagem do n.º de atividades forenses realizadas
Alvo	N.º de atividades forenses realizadas >= N.º de incidentes
Evidência de implementação	Relatório forense
Frequência	Recolha de medições: após ocorrência de incidentes Relatório: um para cada medição, a enviar ao CA;
Partes responsáveis	Chefia Informática: responsável pela gestão da resposta e recuperação de incidentes e pela medição do controlo Equipa Informática: responsável pela aplicação dos procedimentos de resposta e recuperação de incidentes
Fonte de dados	Sistemas, equipamentos, utilizadores
Formato de reporte	Relatório Gráfico circular para situação atual e gráfico linear para representar evolução.

Anexo X - Políticas de segurança

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Última atualização: 22-04-2018

RESUMO

A proteção da informação deverá ser sempre assegurada, seja qual for o seu formato, a forma como é partilhada, comunicada ou armazenada, de modo a garantir a continuidade do negócio e a minimizar os riscos resultantes de ameaças físicas e lógicas.

OBJETIVOS

O objetivo desta política é estabelecer as regras gerais e os princípios para a segurança da informação.

ÂMBITO

Esta política aplica-se a toda a empresa.

POLÍTICA

1. Os riscos de segurança da informação são compreendidos e tratados de acordo com o nível de risco aceite pela empresa.

2. É protegida a confidencialidade da informação de colaboradores, clientes, fornecedores, propriedade intelectual e quaisquer dados sensíveis.

3. É mantida a integridade dos registos informáticos nas bases de dados.

4. É assegurada a disponibilidade da rede de dados da empresa e dos serviços associados.

5. Todos os colaboradores são responsáveis pela segurança da informação utilizada no desempenho das suas funções.

6. A empresa incentiva a aplicação de meios técnicos para a implementação de controlos de segurança da informação nos processos de gestão.

7. Os riscos de segurança da informação serão monitorizados e serão tomadas medidas sempre que ocorram alterações que apresentem riscos não aceitáveis para a empresa.

8. Relatórios do estado de segurança da informação estarão disponíveis para os responsáveis.

9. Possibilidades de fraude associadas ao abuso de sistemas de informação serão levadas em conta na gestão dos sistemas de informação, nomeadamente através de análise aos registos de transações.

10. Não serão permitidas situações que possam colocar a empresa perante violação da lei e dos regulamentos aplicáveis à empresa.

11. As políticas serão transmitidas a todos os colaboradores e será solicitada a tomada de conhecimento.

RESPONSABILIDADES

1. A gestão de topo é responsável por garantir que a segurança da informação é abordada de forma adequada em toda a empresa.

2. A Direção de Serviços é responsável por garantir que os colaboradores na sua dependência protegem a informação de acordo com os padrões e regras da empresa.

3. A Chefia Informática (com responsabilidades de segurança) presta informação à direção e à gestão de topo, apoia a equipa técnica e garante que os relatórios do estado de segurança da informação estão disponíveis.

4. Cada colaborador tem responsabilidades de segurança da informação, como parte do seu trabalho.

HISTÓRICO DE REVISÕES

Data de Revisão	Responsável	Resumo da Revisão
22-04-2018	Serviço de Informática	Definição da política de segurança da informação.

Anexo X - Políticas de segurança

POLÍTICA DE CÓPIA DE SEGURANÇA (BACKUPS)

Última atualização: 24-05-2018

RESUMO

A indisponibilidade de cópias de segurança de dados e de sistemas ou falhas na integridade desses ficheiros pode sujeitar a empresa a problemas graves a nível da continuidade do negócio em caso de necessidade de recuperação de informação.

OBJETIVOS

O objetivo desta política é salvaguardar os ativos de informação da IHM, evitar a perda de dados em caso de eliminação acidental, corrupção dos dados, falha nos sistemas ou desastre, permitir a reposição das informações e processos de negócios, gerir e proteger os processos de *backup*, de reposição e os recursos utilizados no processo.

ÂMBITO

Esta política abrange todos os recursos de sistema e ativos que são propriedade, operados, mantidos e controlados pela IHM e todos os restantes recursos de sistema, internos e externos, que interagem com esses sistemas.

POLÍTICA

Backups de sistema

1. A NAS receberá o *backup* dos controladores de domínio **diariamente** e enviá-lo-á para *tape* encriptada **diariamente**.

2. A NAS receberá as imagens dos sistemas aplicacionais **diariamente** e enviá-las-á para *tape* encriptada **diariamente**.

3. A NAS receberá o *backup* de dados das aplicações **diariamente** e enviá-lo-á para *tape* encriptada **diariamente**.

4. A NAS receberá o *backup* de dados dos utilizadores **semanalmente** e enviá-lo-á para *tape* encriptada **semanalmente**.

5. O reporte dos backups efetuados deve ser enviado pelo técnico ao responsável do serviço informático **semanalmente** e deverá incluir o preenchimento da seguinte tabela (*exemplo*):

Tabela 17 - Reporte de execução de backup (exemplo)

Timestamp início	Timestamp fim	Sist. / App	Tipo de *backup*	Nome do ficheiro	Tamanho do ficheiro	Repositório	Técnico
2405182200	*2405182245*	*App1*	*Completo*	*App1_2405182200.bak*	*48.712 KB*	*NAS + Tape*	*Téc. 1*

Transporte e armazenamento de tapes de backup

6. As *tapes* serão claramente identificadas com um rótulo e armazenadas num espaço seguro apenas acessível ao pessoal técnico.

7. Os *backups* diários serão armazenados *onsite,* num cofre corta-fogo localizado fora do *Data Center*.

8. Os *backups* diários serão mantidos durante uma semana.

9. Os backups semanais serão armazenados *offsite* num espaço seguro apenas acessível ao pessoal técnico.

10. Os backups semanais serão mantidos pelo período de 6 meses.

11. Os *backups* completos em *tape* são retidos durante **1 ano**, salvo requisitos legais específicos.

Verificação de backups

12. As informações registadas sobre os *backups* serão analisadas para verificação e correção de erros, monitorização da duração da tarefa de backup e otimização do desempenho sempre que possível.

13. A verificação da integridade dos *backups* e imagens de sistemas aplicacionais será realizada **semanalmente** e testada em ambiente virtual.

14. Os técnicos documentarão os *backups* e as reposições de teste realizados para demonstrar a conformidade com a política no âmbito de uma auditoria

Recuperação de dados

Em caso de falha grave do sistema, os dados de *backup* serão disponibilizados no prazo de 2 dias úteis após a substituição equipamento destruído.

Em caso de falha não grave do sistema ou erro do utilizador, os dados de *backup* serão disponibilizados aos utilizadores no prazo de 1 dia útil.

Pedidos de reposição de dados

Em situações de eliminação acidental ou corrupção de dados, os pedidos de reposição serão feitos via e-mail ao responsável do serviço informático, que diligenciará.

RESPONSABILIDADES

1. O responsável do serviço informático irá garantir a disponibilização dos recursos humanos e técnicos necessários à realização dos *backups* (pessoal técnico, acesso destes aos sistemas e à NAS e tapes em número suficiente).

2. O responsável do serviço informático é responsável por informar os técnicos sobre esta política.

3. O responsável do serviço informático é responsável por calendarizar, documentar e afetar as tarefas de realização e teste dos *backups* aos técnicos.

4. O responsável do serviço informático é responsável pela verificação do *log* de *backups* para atestar a conclusão da tarefa com sucesso, pela segurança e disponibilidade de todas *tapes* e *logs* de *backup* e pelo acompanhamento dos testes de reposição em ambiente virtual e real.

5. Os técnicos de informática irão garantir que os *backups* são concluídos, reportar e registar a ocorrência de falhas no *backup e* investigar as exceções reportadas pelo sistema.

6. Os técnicos de informática irão verificar a integridade das cópias de segurança realizadas e testar a capacidade de reposição em ambiente virtual.

7. Os técnicos de informática irão acautelar a capacidade dos sistemas de armazenamento das cópias de segurança para salvaguarda da informação durante os períodos definidos.

8. O não cumprimento desta política poderá resultar em ação disciplinar ao infrator, a decidir pela Administração da empresa.

HISTÓRICO DE REVISÕES

Data de Revisão	Responsável	Resumo da Revisão
24-05-2018	Serviço de Informática	Definição da política de *backups*.

Anexo X - Políticas de segurança

POLÍTICA DE CORREIO ELETRÓNICO (E-MAIL)

Última atualização: 27-05-2018

RESUMO

O correio eletrónico é uma ferramenta amplamente utilizada na IHM, sendo uma das principais formas de comunicação entre os diversos serviços e com o exterior. A utilização indevida deste meio de comunicação pode ter consequências de ordem legal, de privacidade e de segurança, pelo que é importante que os utilizadores compreendam a sua adequada utilização.

OBJETIVOS

O objetivo desta política é definir as regras para a utilização do sistema de *e-mail* da IHM, garantir a adequada utilização de contas do domínio ihm.pt e informar os colaboradores sobre a utilização que a IHM considera aceitável e inaceitável deste sistema.

ÂMBITO

Esta política aplica-se a todos os colaboradores que utilizam o sistema de correio eletrónico da IHM através de conta do domínio ihm.pt e a imagem corporativa da empresa nas comunicações estabelecidas.

POLÍTICA

1. Todos os colaboradores da empresa irão ter uma conta de *e-mail* do domínio ihm.pt para as comunicações da empresa.
2. A palavra-passe associada à conta de *e-mail* é comunicada ao colaborador e deve ser alterada por este a partir da primeira utilização.
3. O acesso ao serviço de *e-mail* da IHM pode ser efetuado via *Web*mail, aplicação desktop (e.g. Outlook) e aplicação para dispositivos móveis.
4. Toda o correio eletrónico da IHM deve conter o logotipo e *lettering*, os dados de contato do remetente e o termo de isenção de responsabilidade (*disclaimer*) em rodapé.
5. Todo o correio da IHM deve ser consistente com as políticas e procedimentos da empresa no que respeita a conduta ética, segurança, conformidade com a legislação aplicável e práticas comerciais adequadas.

6. A conta de *e-mail* da IHM deve ser utilizada para as atividades da IHM. A comunicação pessoal é permitida de forma limitada. É proibida a utilização comercial não relacionada com a IHM.
7. Informação da IHM contida numa mensagem de *e-mail* ou num anexo deve ser protegida de acordo com o Regulamento Geral de Proteção de Dados.
8. Devem ser guardados apenas os e-mails que se relacionem com as atividades da empresa.
9. O sistema de correio eletrónico da IHM não deve ser utilizado para a criação ou distribuição de mensagens agressivas, incluindo comentários ofensivos sobre raça, género, deficiência, idade, orientação sexual, pornografia, crenças e práticas religiosas e opções políticas.
10. Colaboradores que recebam *e-mails* com o tipo de conteúdo referido no ponto 5. de qualquer outro colaborador da IHM devem reportar o assunto superiormente imediatamente.
11. Não é permitido o encaminhamento automático de *e-mails* da IHM para sistemas de correio de terceiros. Os *e-mails* pessoais encaminhados pelo colaborador não devem conter informações confidenciais da empresa.
12. Não é permitida a utilização de sistemas de correio eletrónico de terceiros, tais como o Gmail, Yahoo Mail e outros semelhantes, para as atividades da IHM. As comunicações eletrónicas devem ser estabelecidas através dos canais aprovados pela IHM.
13. A utilização de recursos da IHM para o envio e receção de *e-mails* pessoais é aceitável, mas todo o correio não relacionado com o trabalho na empresa deve ser guardado em pastas separadas.

RESPONSABILIDADES

9. Compete aos técnicos de informática a criação e configuração de contas de *e-mail* para novos colaboradores, após receção de comunicação do serviço de recursos humanos.
10. Compete aos técnicos de informática a eliminação de contas de *e-mail* para colaboradores que deixem de ter vínculo laboral com a empresa, após receção de comunicação do serviço de recursos humanos, salvaguardando os respetivos ficheiros de *backup*.
11. Os colaboradores são integralmente responsáveis pelos conteúdos das mensagens por si enviadas.
12. O não cumprimento desta política poderá resultar em ação disciplinar ao infrator, a decidir pela Administração da empresa.

HISTÓRICO DE REVISÕES

Data de Revisão	Responsável	Resumo da Revisão
27-05-2018	Serviço de Informática	Definição da política de correio eletrónico.

Anexo X - Políticas de segurança

POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Última atualização: 28-05-2018

RESUMO

Os desafios atuais à segurança da informação exigem atuação imediata em caso de ataque real ou suspeita de vulnerabilidades que coloquem em causa a confidencialidade, a integridade e disponibilidade da informação. A gestão de incidentes pretende minimizar o risco de perda de dados, a disrupção das atividades, os impactos financeiros e legais graves e os custos de reputação para a empresa.

OBJETIVOS

Esta política define as regras para a gestão e reporte imediato de incidentes de segurança que afetem os sistemas de informação, causem a perda, a divulgação não autorizada e a corrupção de dados e danos em equipamentos.

ÂMBITO

Esta política aplica-se a todos os colaboradores da empresa.

POLÍTICA

1. A IHM irá monitorizar o tráfego na rede e os sistemas aplicacionais para detetar e alertar sobre a ocorrência de ataques de segurança e interrupções nos sistemas, mantendo os registos e as evidências necessárias à investigação exigida legalmente.

2. Todos os colaboradores devem reportar imediatamente, via telefone ou e-mail, quaisquer eventos suspeitos ao responsável do serviço e ao serviço de informática.

3. Os eventos reportados devem conter informação precisa no sentido de ajudar a investigação dos especialistas e agilizar as intervenções.

4. Os técnicos de informática irão analisar o reporte de eventos e determinar se se trata de um incidente, ou remeter a análise para um especialista em caso de dúvida.

5. Os incidentes serão classificados de acordo com a sua criticidade.

6. Se a investigação a um incidente requerer acesso ao computador de um utilizador, por exemplo em caso de suspeita de *download* de *software* ilegal, tal procedimento deve ser validado pelo responsável do serviço informático.

7. O responsável do serviço informático diligenciará a comunicação do incidente à cadeia de comando interna para cumprimento da obrigatoriedade de reporte às autoridades competentes.

8. Os técnicos e especialistas de segurança reunirão para rever o incidente, averiguar se todas as ações tomadas foram as corretas para mitigar o impacto e identificar que outras ações são necessárias para reduzir o risco de futuros ataques semelhantes.

9. O responsável do serviço informático receberá relatórios de todos os incidentes de segurança da informação, que serão registados em processo no sistema de gestão documental, e dará a conhecer à administração da empresa para identificação de lições a serem aprendidas, conhecimento dos padrões de incidentes e prova das vulnerabilidades que precisam ser resolvidas.

RESPONSABILIDADES

13. Compete a todos os colaboradores e prestadores de serviço o reporte de eventos de segurança ou suspeitas de incidentes.

14. Compete aos técnicos de informática e aos especialistas de segurança a análise aos eventos reportados, a determinação se se trata de um incidente de segurança e a aplicação imediata dos planos de resposta e recuperação.

15. Compete aos técnicos de informática e aos especialistas de segurança documentar as operações realizadas e reportar a ocorrência ao responsável do serviço.

16. Compete ao responsável do serviço informático comunicar o incidente à cadeia de comando interna.

10. Compete à administração o cumprimento da obrigatoriedade de reporte às autoridades (Polícia Judiciária e Centro Nacional de Cibersegurança).

17. O não cumprimento desta política poderá resultar em ação disciplinar ao infrator, a decidir pela Administração da empresa.

HISTÓRICO DE REVISÕES

Data de Revisão	Responsável	Resumo da Revisão
28-05-2018	Serviço de Informática	Definição da política de gestão de incidentes de segurança da informação.

Anexo X - Políticas de segurança

POLÍTICA DE INSTALAÇÃO DE SOFTWARE

Última atualização: 22-04-2018

RESUMO

Permitir a instalação de *software* aos colaboradores pode sujeitar a empresa a problemas de exposição a código malicioso e intrusão na rede. *Software* não licenciado pode ser detetado em processos de auditoria, incorrendo a empresa no pagamento de multas avultadas.

OBJETIVOS

O objetivo desta política é definir os requisitos para instalação de *software* nos sistemas de produção da empresa. Pretende-se minimizar o risco de infeção dos sistemas, o risco de perda de informação e de funcionalidades nos programas e o risco de incumprimento legal por utilização de *software* não licenciado.

ÂMBITO

Esta política aplica-se a todos os colaboradores e prestadores de serviços que utilizem equipamentos informáticos da empresa. Estão incluídos todos os computadores *desktop*, portáteis, servidores, *smartphones*, *tablets* e quaisquer outros equipamentos informáticos operados na empresa.

POLÍTICA

1. Apenas podem ser instalados os seguintes programas nos postos de utilizador:
    a. Sistema operativo
    b. Aplicações *Office;*
    c. Aplicações internas, de acordo com o perfil e serviço do utilizador (e.g. ERP para o serviço financeiro);
    d. Plugins necessários ao funcionamento das aplicações
    e. *Browsers* Firefox e IE (apenas para aplicações *legacy*);
    f. Certificados de segurança;
    g. *Drivers* de impressão/digitalização;
    h. Aplicação Autenticação.Gov (leitura do Cartão de Cidadão e assinatura digital);
    i. IDE's para desenvolvimento (só programadores);
    j. Aplicação cliente antivírus + segurança

2. Apenas podem ser instalados os seguintes programas nos servidores:
    a. Sistema operativo
    b. *Software* de virtualização

c. Aplicação servidora
d. Aplicação gestora de base de dados
e. *Plugins* necessários ao funcionamento das aplicações
f. Aplicação cliente antivírus + segurança

3. A instalação de *software* nos equipamentos informáticos operados na rede da empresa apenas pode ser efetuada pelos técnicos afetos ao serviço de Informática ou por prestadores de serviço no âmbito de operações de suporte técnico às aplicações, após validação do software a instalar por parte do coordenador da Informática.

4. Pedidos para instalação de software específico devem ser solicitados, via e-mail, ao Diretor/Chefe do Serviço requisitante que, em caso de aprovação, deverá encaminhar o pedido para o serviço de Informática, pela mesma via.

5. Apenas pode ser instalado *software* presente na lista de programas aprovados pelo Serviço de Informática. Caso o *software* solicitado não exista na empresa, o Serviço de Informática deve analisar o pedido e efetuar requisição interna para o licenciamento, se tal se justificar.

6. Compete ao serviço de Informática diligenciar a aquisição do *software* licenciado necessário às operações informáticas, gerir o licenciamento e os prazos de renovação.

RESPONSABILIDADES

18. Apenas os técnicos afetos ao serviço de Informática podem testar novas aplicações para efeitos de compatibilidade e executar as instalações de *software*.

19. O serviço de Informática irá validar previamente a instalação de *software* por parte de prestadores de serviço.

20. O serviço de Informática irá verificar o cumprimento desta política periodicamente, verificando os equipamentos localmente, utilizando ferramentas de monitorização e reporte, auditorias internas e externas, ou outros mecanismos que considere adequados. Os resultados serão reportados à Administração.

21. O não cumprimento desta política poderá resultar em ação disciplinar ao infrator, a decidir pela Administração da empresa.

HISTÓRICO DE REVISÕES

Data de Revisão	Responsável	Resumo da Revisão
22-04-2018	Serviço de Informática	Definição da política de instalação de *software*.

Anexo X - Políticas de segurança

POLÍTICA DE PALAVRA-PASSE

Última atualização: 23-05-2018

RESUMO

Permitir aos utilizadores e administradores a definição de uma palavra-passe individual, complexa, a ser renovada periodicamente.

OBJETIVOS

O objetivo desta política é definir os requisitos para a definição de palavra-passe de acesso ao domínio e aplicações. Pretende-se um aumento da complexidade das palavras-passe, que dificulte qualquer tentativa de ataque para descoberta de credenciais e consequente acesso indevido.

ÂMBITO

Esta política aplica-se a todos os colaboradores que acedem aos sistemas da empresa no domínio IHM.

POLÍTICA

Construção da palavra-passe

A palavra-passe exige a inclusão de 3 dos 4 seguintes conjuntos de caracteres:

- letras minúsculas (a…z)
- letras maiúsculas (A…Z)
- números (0…9)
- caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /)

Em alternativa, pode ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».

Palavra-passe de utilizador

A palavra-passe de utilizador deve ter no mínimo 9 caracteres e ser complexa.

A palavra-passe tem validade de 180 dias, devendo ser definida outra pelo utilizador, diferente de todas as anteriormente utilizadas.

Palavra-passe de administrador

A palavra-passe de administrador deve ter no mínimo 13 caracteres e ser complexa.

O acesso de administrador exigirá autenticação *dual-factor*: palavra-passe + código recebido via SMS.

A palavra-passe tem validade de 180 dias, devendo ser definida outra pelo administrador, diferente de todas as anteriormente utilizadas.

RESPONSABILIDADES

22. O administrador do domínio irá refletir as regras aqui definidas na política de domínio, para aplicação automática a todos os utilizadores.

23. Os utilizadores e administradores são responsáveis pela confidencialidade da sua palavra-passe, não devendo revelá-la ou deixá-la exposta em nenhuma circunstância.

24. O não cumprimento desta política por parte dos utilizadores poderá resultar em perda de acesso ao domínio e consequente impossibilidade de acesso às aplicações.

25. O não cumprimento desta política por parte de utilizadores com acessos privilegiados (administradores) poderá resultar em ação disciplinar ao infrator, a decidir pela Administração da empresa.

HISTÓRICO DE REVISÕES

Data de Revisão	Responsável	Resumo da Revisão
23-05-2018	Serviço de Informática	Definição da política de palavra-passe.

Anexo X - Políticas de segurança

POLÍTICA DE SEGURANÇA DE REDE

Última atualização: 22-04-2018

RESUMO

A infraestrutura de rede é uma componente critica para a utilização dos sistemas de informação da IHM, sem a qual não é possível efetuar a maioria das operações necessárias ao normal funcionamento da empresa. Quaisquer dispositivos que sejam ligados à rede deverão estar em conformidade com as políticas da IHM.

OBJETIVOS

O objetivo desta política é proteger a integridade da rede da IHM, reduzir os riscos e perdas associados a ameaças de segurança aos recursos de informação e garantir o acesso seguro e confiável aos colaboradores, prestadores de serviços e demais entidades que necessitem de acesso à rede da IHM. Pretende também impedir o acesso não autorizado a dados institucionais, de pesquisa e pessoais.

ÂMBITO

Esta política aplica-se a todas as redes da IHM, tanto ao perímetro quanto à infraestrutura e a todos os colaboradores, prestadores de serviços, clientes e quaisquer outras entidades que possam efetuar ligações à rede. Estão também abrangidos por esta política todos os dispositivos eletrónicos utilizados por essas pessoas para acesso à rede. Estes dispositivos incluem mas não estão limitados a computadores *desktop* e portáteis, *tablets*, *smartphones*, servidores, consolas, controladores e qualquer outro dispositivo de computação com capacidade de comunicação.

POLÍTICA

Controlos de rede

1. Todas as redes da IHM são instaladas e mantidas pelo serviço informático e suportadas pelos contratos em vigor com os prestadores de serviços.
2. Não é permitida a utilização de equipamentos de rede para além dos equipamentos da empresa.
3. Não é permitida a instalação de qualquer dispositivo ou programa que tenha o potencial de interromper o serviço de rede.
4. Todos os dispositivos com fios ligados às redes da IHM devem ser registados no serviço informático aquando da primeira ligação. Isto aplica-se a impressoras, computadores,

equipamentos de teste e quaisquer dispositivos de comunicação que utilizam protocolos de rede TCP/IP.

5. Todo e qualquer dispositivo ligado à rede que não tenha sido autorizado e registado está sujeito a ser desligado sem aviso prévio, interrompa este algum serviço de rede ou não.
6. Todos os *hosts* ligados às redes internas da IHM terão nomes DNS atribuídos pelo serviço informático.
7. Todos os *hosts* nas redes internas da IHM devem obter e utilizar um endereço IP estático.
8. Não é permitida a configuração de contas de utilizador local nos *routers*.
9. Todos os *routers* terão o serviço *ip directed-broadcast* desativado.
10. Somente os colaboradores, os prestadores de serviços especificamente autorizados e os auditores podem ter acesso às redes internas da IHM.
11. Todas as tentativas de acesso à rede serão registadas e mantidas para auditoria.
12. A credencial de utilizador para acesso à rede deve identificar exclusivamente um único utilizador para garantir a responsabilidade individual nos *logs* do sistema (IP e *hostname*). Não é permitida a utilização de credenciais partilhadas ou de grupo.
13. A entrada de pacotes com endereços de origem inválidos nos *routers* será desativada.
14. As comunicações de rede entre os clientes de *e-mail* e o servidor serão efetuadas através de SSL ou TLS de modo que a transação que ocorre na sessão de autenticação seja protegida.

Acesso remoto

15. O acesso remoto a equipamentos da rede deve ser seguro e controlado, sendo sempre exigida autenticação com palavra-passe.
16. Os colaboradores e os prestadores de serviços com privilégios de acesso remoto são responsáveis pelas ligações que efetuam.
17. Todos os *hosts* ligados remotamente à rede interna da IHM devem utilizar o software de antivírus adquirido pela empresa.
18. A administração remota de equipamentos deve ser executada através de canais seguros (e.g. ligações encriptadas utilizando SSH ou IPSEC) e apenas por pessoal técnico da empresa.

Ligações ao exterior

19. Todas as ligações a redes externas têm de passar pela *firewall*.

20. Não é permitida a ligação de rede com organismos externos, através da Internet ou de qualquer outra rede pública, exceto se que essa ligação tiver sido autorizada pela administração.

21. Os dispositivos ligados à rede wireless são registados para acesso aos serviços de rede.

Ligações VPN

22. Ao utilizar a tecnologia VPN com equipamento pessoal, os colaboradores compreendem que os seus computadores são uma extensão da rede e, como tal, estão sujeitos às mesmas regras e regulamentos que se aplicam aos equipamentos propriedade da IHM e devem ser configurados para cumprir com as Políticas de Segurança da empresa.

23. É responsabilidade dos colaboradores com privilégios de acesso à VPN garantir que utilizadores não autorizados não tenham acesso à rede interna da empresa.

24. Os colaboradores a quem seja permitida a utilização de computadores que não são propriedade da IHM, são responsáveis por configurar o equipamento em conformidade com as políticas VPN e de rede da empresa.

25. Quando ligado à rede da empresa, a VPN forçará todo o tráfego de e para o computador através do túnel VPN. Todo restante tráfego será ignorado.

26. Os utilizadores das VPN serão desligados automaticamente da rede após 30 minutos de inatividade. O utilizador deverá efetuar o login novamente para voltar a ligar-se à rede.

27. Não devem ser utilizados comandos *ping* ou outras técnicas de comunicação na rede para manter a ligação remota aberta.

RESPONSABILIDADES

Compete aos técnicos de informática:

- Gerir e manter os equipamentos de rede.
- Monitorizar, registar e analisar o tráfego de rede para garantir a conformidade com as políticas de segurança.
- Identificar, avaliar e resolver as vulnerabilidades de segurança, as violações e ameaças aos recursos.
- Planear, implementar e manter VPNs.
- Gerir a infraestrutura de rede, os equipamentos com e sem fios, servidores, aplicações e qualquer sistema com serviços de rede.
- Proteger as ligações com outros organismos.

HISTÓRICO DE REVISÕES

Data de Revisão	Responsável	Resumo da Revisão
22-04-2018	Serviço de Informática	Definição da política de segurança da rede.

Anexo X - Políticas de segurança

POLÍTICA DE TRANSFERÊNCIA DE INFORMAÇÃO

Última atualização: 28-05-2018

RESUMO

Os sistemas da IHM e as plataformas disponibilizadas por prestadores de serviços exigem a transferência segura de dados para garantir a confidencialidade, a integridade e a disponibilidade da informação. Adicionalmente, a interoperabilidade dos sistemas e a necessidade de transferência de informações entre cidadãos e organismos carece do estabelecimento de práticas que garantam o acesso seguro à rede, aos sistemas e aos dados.

OBJETIVOS

O objetivo desta política é definir as regras para a transferência segura de dados entre sistemas internos e servidores, bem como de informações para entidades externas através da rede, minimizando o risco de divulgação não autorizada e o comprometimento dos sistemas envolvidos.

ÂMBITO

Esta política aplica-se a todos os colaboradores e prestadores de serviços da IHM que utilizam a rede e os sistemas informáticos da empresa e que produzem e transferem informação digital. São parte integrante desta política todos os sistemas que contêm componentes de tecnologia, aplicações e informações da IHM, incluindo plataformas de terceiros e em particular os sistemas críticos de gestão.

POLÍTICA

1. Utilizar protocolos seguros para transmissão de dados. Se tal não for possível, utilizar técnicas de encapsulamento seguro (IPSec ou SSL em VPN) para impedir que as informações sejam transmitidas em texto livre.

2. A transferência de dados entre a IHM e os prestadores de serviços deve ocorrer em túnel seguro.

3. Se não for possível implementar o encapsulamento seguro de dados, o sistema de destino deve ser completamente isolado da ligação à rede principal (e.g. através de segregação VLAN). O acesso deverá ser restrito a um único IP e as portas específicas a abrir devem servir unicamente para a realização de comunicações legítimas.

4. A segurança da transmissão e testes para detetar possíveis vulnerabilidades devem ser realizados periodicamente para garantir o funcionamento adequado das comunicações.

5. Ficheiros enviados individualmente ou compactados devem ser encriptados com AES256 (por exemplo, utilizando o 7-zip) e utilizando uma palavra-passe que cumpra com a política de palavra-passe da IHM.

6. Um ficheiro encriptado com AES256 pode ser enviado através de uma rede aberta, por exemplo *e-mail*.

7. A palavra-passe do ficheiro encriptado deve ser enviada por outro meio seguro (e.g. SMS)

8. A transferência de ficheiros na IHM implica a sujeição destes a deteção automática de *malware* seja qual for o destino da informação.

9. Informação a ser transferida através de dispositivos móveis, tais como CD, DVD, pen USB, disco rígido externo, entre outros, devem ser gravados nesses dispositivos de forma encriptada (e.g. utilizando compactação encriptada) ou os próprios dispositivos devem ser encriptados (e.g. utilizando o BitLocker).

RESPONSABILIDADES

1. Os colaboradores na posse de informação da IHM são responsáveis por garantir que todas as informações confidenciais são identificadas corretamente e transferidas de acordo com esta política, com as leis aplicáveis e com os contratos em vigor.

2. O serviço de informática é responsável por disponibilizar os programas de encriptação, assegurar a transferência encriptada adequada entre sistemas internos e externos.

HISTÓRICO DE REVISÕES

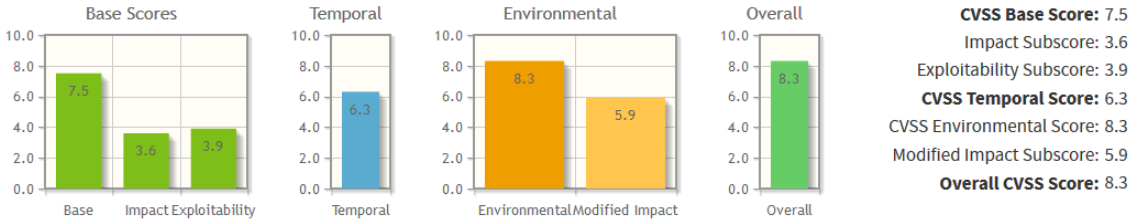
Data de Revisão	Responsável	Resumo da Revisão
28-05-2018	Serviço de Informática	Definição da política de transferência de informação

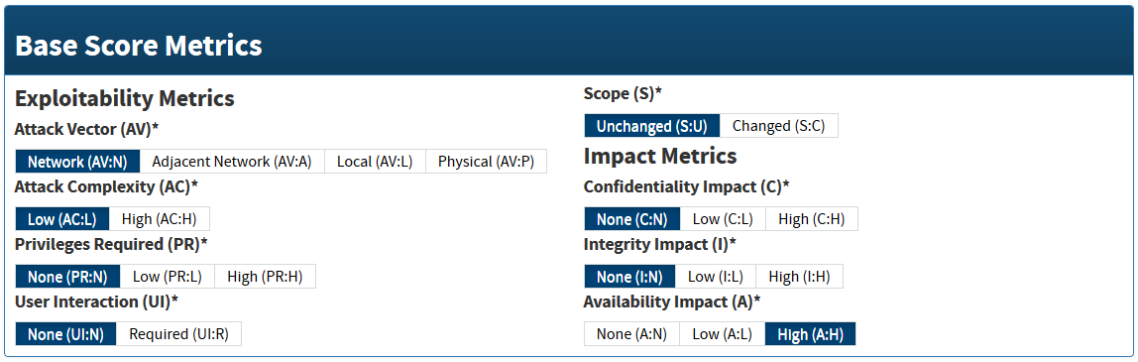
Anexo XI - Checklist de ações para a gestão de incidentes (norma NIST SP 800-61r2)

	Ação	Realizada (S/N)
	Deteção e Análise	
1.	Determinar se ocorreu um incidente	
1.1	Analisar precursores e indicadores	
1.2	Procurar informação correlacionada	
1.3	Pesquisar e investigar (e.g. motores de busca, *knowledge base*)	
1.4	Assim que seja crível que ocorreu um incidente, iniciar a documentação da investigação e a recolha de evidências	
2.	Estabelecer prioridades para lidar com o incidente, de acordo com fatores relevantes: impacto funcional, impacto na informação, esforço de recuperação, etc.	
3.	Reportar o incidente às unidades internas adequadas e a organizações externas (por imposição legal)	
	Contenção, Erradicação e Recuperação	
4.	Obter, preservar, assegurar e documentar as evidências	
5.	Conter o incidente	
6.	Erradicar o incidente	
6.1	Identificar e mitigar todas as vulnerabilidades que foram exploradas	
6.2	Remover o malware e qualquer outro software não apropriado	
6.3	Se outros hosts afetados forem descobertos, repetir as etapas 1.1 e 1.2 da Deteção e Análise para identificar esses hosts, e depois conter (5) e erradicar (6) o incidente nesses hosts	
7.	Recuperar do incidente	
7.1	Repor o funcionamento normal nos sistemas afetados	
7.2	Confirmar que os sistemas afetados estão a funcionar normalmente	
7.3	Se necessário, implementar medidas adicionais de monitorização nos sistemas	
	Atividades Pós-Incidente	
8.	Elaborar relatório de acompanhamento (*follow-up*)	
9.	Organizar uma reunião para discussão das lições aprendidas	

Anexo XII - Common Vulnerability Scoring System Calculator

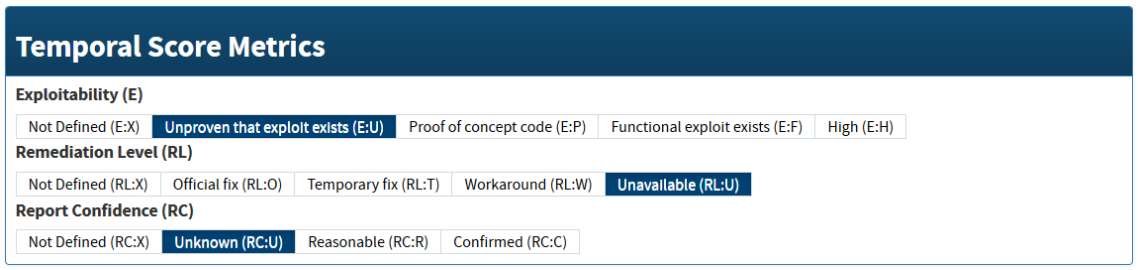
Exemplo de cálculo da gravidade de uma vulnerabilidade, utilizando a CVSS:



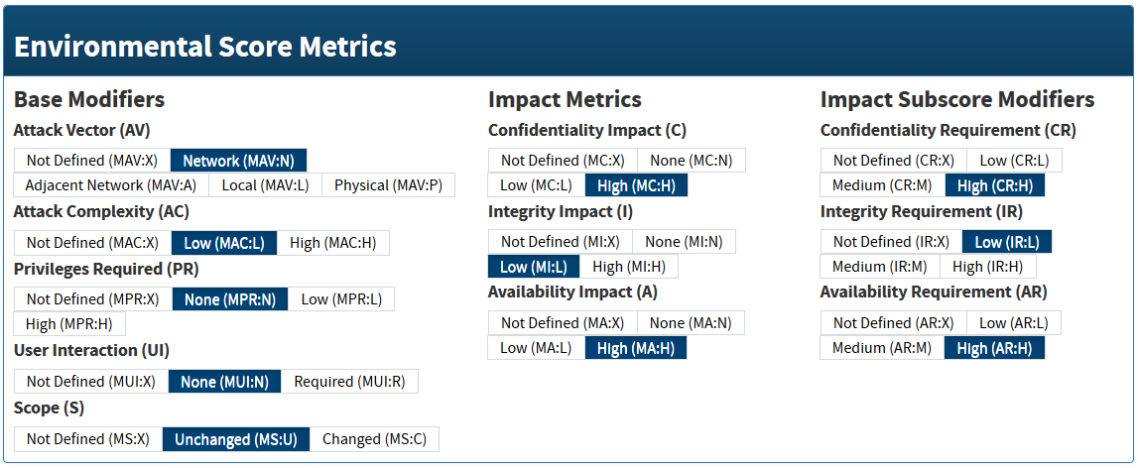


O grupo *Base Score Metric* representa as caraterísticas intrínsecas de uma vulnerabilidade que são constantes ao longo do tempo e abrangem todos os ambientes de utilizador. É composto por dois conjuntos de métricas:

- *Exploitability Metrics*, que reflete a facilidade e os meios técnicos através dos quais a vulnerabilidade pode ser explorada. Isto é, são métricas que representam caraterísticas do que é vulnerável, ou seja, a componente vulnerável.
- *Impact Metrics*, que reflete a consequência direta de uma exploração concretizada e representa a consequência para "aquilo" que sofre o impacto, ou seja, a componente impactada.



As métricas temporais (*Temporal Score Metrics*) medem o estado atual das técnicas de exploração ou disponibilidade de código, a existência de *patches* ou "remedeios", ou a confiança na descrição da vulnerabilidade. Estas métricas mudam ao longo do tempo.



As *Environmental Score Metrics* permitem ao analista personalizar o resultado CVSS dependendo da importância dos bens informáticos afetados, medidos em termos de controlos de segurança complementares/alternativos aplicados, confidencialidade, integridade e disponibilidade. As métricas são o equivalente modificado das métricas base e são atribuídos valores de acordo com a localização da componente na infraestrutura da organização [68].

Legenda:

Base Score Metrics

Attack Vector (AV)

Network – a componente vulnerável está conectada à estrutura de rede. O atacante explora a camada 3 (rede) do OSI. A vulnerabilidade é 'explorável remotamente' (e.g. ataque a um ou mais "*hops*" de distância).

Adjacent Network - a componente vulnerável está conectada à estrutura de rede, contudo o ataque está limitado à mesma rede física (e.g. Bluetooth, IEEE 802.11) ou lógica (e.g. sub-rede local) e não pode ser executado sobre um equipamento da camada 3 do OSI (e.g. router).

Local - a componente vulnerável não está conectada à estrutura de rede. O atacante explora as capacidades de leitura/escrita/execução. O atacante pode estar logado localmente ou pode tirar partido das interações do utilizador para executar código malicioso.

Physical – requer que o atacante aceda fisicamente ou manipule a componente vulnerável (e.g. ligar um periférico a um sistema).

Attack Complexity (AC)

Low – Não existem condições de acesso específicas. O atacante pode esperar obter sucesso repetidamente ao explorar a componente vulnerável.

High - O sucesso do ataque depende de condições fora do controlo do atacante. O atacante tem de fazer um esforço considerável para prepará-lo e executá-lo contra a componente vulnerável.

Privileges Required (PR)

None – O atacante não possui quaisquer privilégios antes do ataque, não requerendo qualquer acesso a definições ou ficheiros para desencadear o ataque.

The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files to carry out an attack.

Low – O atacante possui privilégios que lhe dão capacidades básicas de utilização que normalmente apenas afetam configurações e ficheiros de que é proprietário. Este tipo de atacante pode conseguir causar impacto, mas apenas em recursos não sensíveis.

High – O atacante possui privilégios que lhe dão controlo significativo (e.g. administrativo) sobre a componente vulnerável, que pode afetar configurações e ficheiros.

User Interaction (UI)

None – O sistema vulnerável pode ser explorado sem interação de qualquer utilizador.

Required – A exploração de uma vulnerabilidade requer que o utilizador efetue uma ação antes da vulnerabilidade poder ser explorada (e.g. o utilizador tem de clicar num link num e-mail).

Scope (S)

Unchanged – Uma vulnerabilidade explorada apenas afeta recursos geridos pela mesma autoridade. Neste caso, a componente vulnerável e a componente impactada são as mesmas.

Changed - Uma vulnerabilidade explorada pode afetar recursos para além dos privilégios de autorização pretendidos pela componente vulnerável. Neste caso, a componente vulnerável e a componente impactada são diferentes.

Confidentiality Impact (C)

None – Não há perda de confidencialidade na componente impactada.

Low – Há alguma perda de confidencialidade. É obtido acesso a alguma informação restrita mas o atacante não tem controlo sobre a informação obtida, ou a extensão da perda é restrita. A revelação da informação não causa uma perda grave e direta à componente impactada.

High – Há perda total de confidencialidade, resultando em todos os recursos na componente impactada serem divulgados ao atacante. Alternativamente, é obtido acesso a apenas alguma informação restrita, mas a informação revelada representa um impacto grave e direto.

Integrity Impact (I)

None – Não há perda de integridade na componente impactada.

Low – A modificação de dados é possível, mas o atacante não tem controlo sobre a consequência da modificação, ou a extensão da modificação é restrita. A modificação de dados não tem um impacto grave e direto na componente impactada.

High – Há perda total de integridade, ou perda completa de proteção (e.g. o atacante consegue modificar algum/todos os ficheiros protegidos pela componente impactada. Alternativamente, apenas alguns ficheiros podem ser modificados, mas a modificação maliciosa teria consequências graves e diretas na componente impactada.

Availability Impact (A)

None – Não há impacto na disponibilidade na componente impactada.

Low – O desempenho é reduzido ou ocorrem interrupções na disponibilidade de recursos. Mesmo que a exploração repetida da vulnerabilidade seja possível, o atacante não tem capacidade de negar completamente o serviço a utilizadores legítimos. Os recursos na componente impactada estão parcialmente disponíveis o tempo todo, ou totalmente disponíveis apenas algum tempo, mas não há consequências graves e diretas na componente impactada.

High – Há perda total de disponibilidade, resultante do atacante ser capaz de negar completamente o acesso aos recursos na componente impactada; esta perda é mantida (enquanto o atacante continua o ataque) ou é persistente (a condição persiste mesmo após o ataque ter terminado). Alternativamente, o atacante tem a capacidade de negar alguma disponibilidade, mas a perda de disponibilidade representa uma consequência grave e direta sobre a componente impactada (e.g. o atacante não pode interromper ligações existentes mas consegue impedir novas ligações; o atacante pode explorar repetidamente a vulnerabilidade que, em cada instância de um ataque com sucesso, deixa vazar apenas uma pequena quantidade de memória, mas que depois de repetidas explorações causa a total indisponibilidade do serviço).

Temporal Score Metrics

Exploitability (E)

Not Defined – Atribuir este valor à métrica não influencia o resultado.

Unproven that exploit exists – Não há código de exploração disponível, ou a exploração é inteiramente teórica.

Proof of concept code – Código de exploração demonstrável está disponível, ou uma demonstração de ataque não é praticável para a maioria dos sistemas. O código ou técnica não é funcional em todas as situações e pode requerer modificação substancial por um atacante hábil.

Functional exploit exists – Código de exploração funcional está disponível. O código funciona na maioria das situações onde a vulnerabilidade exista.

High – Código autónomo e funcional existe, ou não é necessária exploração (*trigger* manual) e os detalhes estão largamente disponíveis. Código de exploração funciona em todas as situações, ou está a ser entregue ativamente através de um agente autónomo (e.g como um *worm* ou vírus). Sistemas em rede devem registar tentativas de *scanning* e exploração. O desenvolvimento da exploração atingiu o nível confiável, está largamente disponível e dispõe de ferramentas automatizadas fáceis de utilizar.

Remediation Level (RL)

Not Defined – Atribuir este valor à métrica não influencia o resultado.

Official fix – Uma solução completa de fornecedor está disponível. O fornecedor emitiu um *patch* oficial, ou um *upgrade* está disponível.

Temporary fix – Existe uma correção oficial disponível, mas temporária. Isto inclui as ocorrências em que o fornecedor emite uma correção temporária, uma ferramenta ou uma solução alternativa.

Workaround – Existe uma solução não oficial que não é disponibilizada pelo fornecedor. Em alguns casos, os utilizadores da tecnologia afetada criam o seu próprio *patch* ou providenciam os passos para uma solução alternativa ou para mitigar a vulnerabilidade.

Unavailable – Não existe solução disponível ou esta é impossível de aplicar.

Report Confidence (RC)

Not Defined – Atribuir este valor à métrica não influencia o resultado.

Unknown – Há relatórios de impacto que indicam a presença da vulnerabilidade. Os relatórios indicam que a causa da vulnerabilidade é desconhecida, ou os relatórios diferem na causa ou impacto da vulnerabilidade. A verdadeira natureza da vulnerabilidade é desconhecida, e há pouca confiança na validação dos relatórios ou se um resultado básico estático pode ser aplicado dadas as diferenças descritas.

Reasonable – Detalhes significativos são divulgados, mas os analistas não têm confiança absoluta sobre a raiz da causa, ou não têm acesso ao código fonte para confirmar todas as interações que podem levar ao resultado. Existe um nível de confiança razoável, contudo, de que o bug é reproduzível e pelo menos um impacto é passível de verificação (e.g. através de explorações demonstráveis).

Confirmed – Existem relatórios detalhados, ou a reprodução funcional é possível (e.g. através de explorações funcionais). O código fonte está disponível para verificação independente das asserções dos analistas, ou o autor ou fornecedor do código afetado confirmou a presença da vulnerabilidade.

Environmental Score Metrics (Impact Subscore Modifiers)

Confidentiality Requirements (CR)

Not Defined – Atribuir este valor à métrica não influencia o resultado.

Low – A perda de confidencialidade deve ter apenas um efeito adverso limitado na organização ou indivíduos associados à organização (e.g. colaboradores, clientes).

Medium - A perda de confidencialidade deve ter um efeito adverso grave na organização ou indivíduos associados à organização (e.g. colaboradores, clientes).

High – A perda de confidencialidade deve ter um efeito adverso catastrófico na organização ou indivíduos associados à organização (e.g. colaboradores, clientes).

Integrity Requirements (IR)

Not Defined – Atribuir este valor à métrica não influencia o resultado.

Low – A perda de integridade deve ter apenas um efeito adverso limitado na organização ou indivíduos associados à organização (e.g. colaboradores, clientes).

Medium - A perda de integridade deve ter um efeito adverso grave na organização ou indivíduos associados à organização (e.g. colaboradores, clientes).

High – A perda de integridade deve ter um efeito adverso catastrófico na organização ou indivíduos associados à organização (e.g. colaboradores, clientes).

Availability Requirements (AR)

Not Defined – Atribuir este valor à métrica não influencia o resultado.

Low – A perda de disponibilidade deve ter apenas um efeito adverso limitado na organização ou indivíduos associados à organização (e.g. colaboradores, clientes).

Medium - A perda de disponibilidade deve ter um efeito adverso grave na organização ou indivíduos associados à organização (e.g. colaboradores, clientes).

High – A perda de disponibilidade deve ter um efeito adverso catastrófico na organização ou indivíduos associados à organização (e.g. colaboradores, clientes).

Anexo XIII - Resultados da medição dos controlos

As medições dos controlos foram realizadas de acordo com os critérios definidos no *Anexo IX - Monitorização e medição da eficácia dos controlos*.

Na sequência apresenta-se a tabela com as secções, respetivos controlos e resultados obtidos, realçados com a cor correspondente ao resultado, quando aplicável:

Secção	Medida	Resultado	Alerta
A.5.1.1	Percentagem de políticas estabelecidas.	(4/8) * 100 = 50%	
A.12.1.1	Número de procedimentos documentados e disponibilizados.	1	
A.12.1.2	Percentagem de novas aplicações desenvolvidas em cumprimento com as boas práticas de gestão de alterações.	(0/1) * 100 = 0%	
A.12.1.3	Percentagem de capacidade em disco disponível em cada sistema.	Sistema A: (15/135) * 100 = 11,11%	
		Sistema B: (42/135) * 100 = 31,11%	
		Sistema C: (199/300) * 100 = 66,33%	
		Sistema D: (1140/2000) * 100 = 72%	
		Sistema E: (72/145) * 100 = 49,65%	
		Sistema F: (38/300) * 100 = 12,66%	
		Sistema G: (590/10000) * 100 = 5,90%	
		Sistema H: (970/2400) * 100 = 40,41%	
		Sistema I: (55/72) * 100 = 76,38%	
A.12.1.4	Percentagem de ambientes por aplicação	Aplicação 1: (1/3) * 100 = 33,33%	
		Aplicação 2: (1/3) * 100 = 33,33%	
		Aplicação 3: (1/3) * 100 = 33,33%	
		Aplicação 4: (1/3) * 100 = 33,33%	

		Aplicação 5: (1/3) * 100 = 33,33%	
		Aplicação 6: (2/3) * 100 = 66,66%	
A.12.2.1	Número de ataques detetados que não foram bloqueados pelo sistema.	0	
	Percentagem de utilizadores que participaram em ações de consciencialização.	Proteção contra *ransomware*: (126/126) * 100 = 100%	
		Proteção de Dados no Sistema A: (6/28) * 100 = 21,42%	
A.12.3.1	Percentagem dos dados e sistemas que necessitando ser repostos, são repostos em 48h (max.).	Não houve necessidade de reposição de dados ou sistemas durante a fase de implementação.	
A.12.4.1	Número de *logs* de auditoria revistos por período de tempo, por sistema.	Sistema A: (0/35) * 100 = 0%	
		Sistema B: (1/18) * 100 = 5,55%	
		Sistema C: (4/38) * 100 = 10,52%	
		Sistema D: (11/72) * 100 = 15,27%	
		Sistema E: (5/67) * 100 = 7,46%	
		Sistema F: (0/35) * 100 = 0%	
		Sistema G: (6/84) * 100 = 7,14%	
		Sistema H: (3/36) * 100 = 8,33%	
		Sistema I: (2/47) * 100 = 4,25%	
A.12.4.2	N.º de registos com atributos modificados. N.º de registos com *hash* modificado.	Sistemas A a I: 0 atributos modificados. Sem medições	
A.12.4.3	Percentagem de atividades dos administradores e operadores de sistemas por período de tempo.	Não foi possível efetuar a medição por não haver registos em sistema. A maioria das atividades são de conhecimento tácito, sendo realizadas sem registo. A contagem de atividades atribuídas via *e-mail* não se traduz num resultado fidedigno face à falta de registos mencionada.	

A.12.4.4	Percentagem de relógios sincronizados com uma única referência horária.	(138 / 156) * 100 = 88,46%	
A.12.5.1	Percentagem de *software* licenciado.	(38/38) * 100 = 100%	
A.12.6.1	Percentagem de equipamentos configurados de acordo com as políticas.	Não foi possível determinar porque o levantamento desta informação está em curso, atendendo ao elevado número de equipamentos.	
	Percentagem de sistemas críticos com avaliação de vulnerabilidades realizada desde a última grande *release*.	100% Por motivos de confidencialidade não é possível indicar o número de sistemas críticos.	
	Quantificação das vulnerabilidades não corrigidas nos sistemas críticos (*unpatched*), calculada através do *Common Vulnerability Scoring System Calculator (Version 3).*	Não houve vulnerabilidades não corrigidas.	
A.12.6.2	Percentagem de software instalado pelos utilizadores.	[(0/126*38)] * 100 = 0%	
A.12.7.1	Tempo de inatividade dos serviços devido a realização de auditoria.	Não foi realizada nenhuma auditoria durante o período de realização deste trabalho.	
A.13.1.1	Regras sem utilização na *firewall.*	0	
	Servidores *Web* fora da DMZ com dupla *firewall.*	0	
	Percentagem de *switches* com *software* de gestão efetivamente utilizado.	> 80% Por motivos de confidencialidade não é possível indicar o número de *switches*.	
	Percentagem de tentativas de intrusão bloqueadas.	> 80% Por motivos de confidencialidade não é possível indicar o número de tentativas de intrusão.	
	Percentagem de equipamentos com *firmware* atualizado.	>=40% e <=80% Por motivos de confidencialidade não é possível indicar o número de	

		equipamentos com *firmware* atualizado.	
	Percentagem de registos estáticos de IP e MAC *Address* nos *switches.*	> 80% Por motivos de confidencialidade não é possível detalhar esta informação.	
A.13.1.2	Percentagem de serviços de rede não necessários.	Não foi possível determinar porque o levantamento desta informação está em curso, atendendo ao elevado número de equipamentos.	
	Percentagem de *APs* com SSID oculto.	>=40% e <=80% Por motivos de confidencialidade não é possível indicar o número de APs.	
	Percentagem de *APs* configurados com WPA2 802.11i.	> 80% Por motivos de confidencialidade não é possível detalhar esta informação.	
	Percentagem de dispositivos *Bluetooth* com *auto-discovery* ativado.	> 80% Por motivos de confidencialidade não é possível detalhar esta informação.	
	Percentagem de zonas DNS protegidas com DNSSEC.	Sem medição.	
A.13.1.3	Percentagem de acessos indevidos a VLANs.	Sem medição.	
	Pedidos de acesso entre sistemas residentes no mesmo *hypervisor.*	Sem medição.	
A.13.2.1	Percentagem de ligações de dados não encriptadas.	< 20% Por motivos de confidencialidade não é possível detalhar esta informação.	
	Percentagem de aplicações *Web* com estabelecimento de sessão segura.	>=40% e <=80% Por motivos de confidencialidade não é possível detalhar esta informação.	
A.13.2.2	Percentagem de protocolos que impõem a transferência segura da informação.	< 40% Por motivos de confidencialidade não é possível detalhar esta informação.	
A.13.2.3	N.º de certificados de encriptação/autenticação por aplicação com funcionalidades de *e-mail.*	Aplicação 7: 1 certificado	
		Aplicação 8: 30 certificados	
		Aplicação 9: 6 certificados	
		Aplicação 10: 0 certificados	
A.13.2.4	Percentagem de acordos de confidencialidade e de não divulgação que são cumpridos.	(1/1) * 100 = 100%	

A.16.1.1	Percentagem de planos de resposta e de recuperação em conformidade.	(0/1) * 100 = 0%	
	Papéis atribuídos e ordem de intervenção.	Não houve atribuição de responsabilidades.	
A.16.1.2	Número de incidentes reportados num ano.	(0/3) * 100 = 0%	
A.16.1.3	Percentagem de reportes de pontos fracos.	(1/2) * 100 = 50%	
A.16.1.4	Percentagem de avaliações realizadas.	(8/41) * 100 = 19,5%	
	Percentagem de incidentes categorizados.	(2/3) * 100 = 66,66%	
A.16.1.5	Percentagem de execução do plano de resposta num evento.	(0/3610) * 100 = 0%	
A.16.1.6	Percentagem de incidentes após início de partilha de informações.	(1/3) * 100 = 33,33%	
	Percentagem de processos de deteção melhorados.	(9/9) * 100 = 100% • Processo de classificação de programas • Processos de deteção de ameaças: 1. Vírus e *spyware* 2. Ficheiros suspeitos 3. Ferramentas de *hacking* e PUPs 4. URLs de *malware* 5. *Phishing* e fraude 6. Tentativas de intrusão 7. Dispositivos bloqueados 8. *Cookies* de controlo	
	Planos de resposta melhorados.	0	
A.16.1.7	Atividade forense realizada.	0	

Anexo XIV - Resultados (aplicação do Modelo de Capacidade de Processos COBIT 5)

Controlo	Nível (0 a 5)	Capacidade do Processo (0 – Incompleto/Não implementado, 1 - Executado, 2 - Gerido, 3 - Estabelecido, 4 - Previsível, 5 - Otimizado)	Escala (N - Não atingido, P - Parcialmente atingido, L - Amplamente atingido, F - Plenamente atingido)
A.5.1.1 – Políticas para a segurança da informação	0	Incompleto	P - Parcialmente atingido
A.5.1.2 - Revisão das políticas para a segurança da informação	0	Não implementado	N – Não atingido
A.12.1.1 – Procedimentos de operação documentados	0	Incompleto	P - Parcialmente atingido
A.12.1.2 – Gestão de alterações	0	Incompleto	P - Parcialmente atingido
A.12.1.3 – Gestão da capacidade	0	Incompleto	P - Parcialmente atingido
A.12.1.4 – Separação entre ambientes de desenvolvimento, teste e de produção	0	Incompleto	P - Parcialmente atingido
A.12.2.1 – Controlos contra código malicioso (1 de 2)	0	Incompleto	P - Parcialmente atingido
A.12.2.1 – Controlos contra código malicioso (2 de 2)	0	Incompleto	P - Parcialmente atingido
A.12.3.1 – Salvaguarda de informação	1	Executado	L – Amplamente atingido
A.12.4.1 – Registos de eventos	0	Incompleto	P - Parcialmente atingido
A.12.4.2 – Proteção da informação registada	0	Incompleto	P - Parcialmente atingido
A.12.4.3 – Registos de administrador e de operador	0	Não implementado	N – Não atingido
A.12.4.4 – Sincronização de relógio	0	Incompleto	P - Parcialmente atingido
A.12.5.1 – Instalação de software nos sistemas de produção	1	Executado	L – Amplamente atingido
A.12.6.1 – Gestão de vulnerabilidades técnicas (1 de 3)	0	Incompleto	P – Parcialmente atingido
A.12.6.1 – Gestão de vulnerabilidades técnicas (2 de 3)	0	Incompleto	P – Parcialmente atingido
A.12.6.1 – Gestão de vulnerabilidades técnicas (3 de 3)	0	Não implementado	N – Não atingido
A.12.6.2 – Restrições sobre a instalação de software	1	Executado	L – Amplamente atingido

Anexo XIV - Resultados (aplicação do Modelo de Capacidade de Processos COBIT 5)

Controlo	Nível (0 a 5)	Capacidade do Processo (0 – Incompleto/Não implementado, 1 - Executado, 2 - Gerido, 3 - Estabelecido, 4 - Previsível, 5 - Otimizado)	Escala (N - Não atingido, P - Parcialmente atingido, L - Amplamente atingido, F - Plenamente atingido)
A.12.7.1 – Controlos de auditoria nos sistemas de informação	0	Não implementado	N – Não atingido
A.13.1.1 – Controlos da rede (1 de 6)	0	Incompleto	P – Parcialmente atingido
A.13.1.1 – Controlos da rede (2 de 6)	0	Não implementado	N – Não atingido
A.13.1.1 – Controlos da rede (3 de 6)	0	Incompleto	P – Parcialmente atingido
A.13.1.1 – Controlos da rede (4 de 6)	0	Incompleto	P – Parcialmente atingido
A.13.1.1 – Controlos da rede (5 de 6)	0	Incompleto	P – Parcialmente atingido
A.13.1.1 – Controlos da rede (6 de 6)	0	Incompleto	P – Parcialmente atingido
A.13.1.2 – Segurança de serviços de rede (1 de 5)	0	Incompleto	P – Parcialmente atingido
A.13.1.2 – Segurança de serviços de rede (2 de 5)	0	Incompleto	P – Parcialmente atingido
A.13.1.2 – Segurança de serviços de rede (3 de 5)	0	Incompleto	P – Parcialmente atingido
A.13.1.2 – Segurança de serviços de rede (4 de 5)	0	Incompleto	P – Parcialmente atingido
A.13.1.2 – Segurança de serviços de rede (5 de 5)	0	Não implementado	N – Não atingido
A.13.1.3 – Segregação das redes (1 de 2)	0	Não implementado	N – Não atingido
A.13.1.3 – Segregação das redes (2 de 2)	0	Não implementado	N – Não atingido

Anexo XIV - Resultados (aplicação do Modelo de Capacidade de Processos COBIT 5)

Controlo	Nível (0 a 5)	Capacidade do Processo (0 – Incompleto/Não implementado, 1 - Executado, 2 - Gerido, 3 - Estabelecido, 4 - Previsível, 5 - Otimizado)	Escala (N - Não atingido, P - Parcialmente atingido, L - Amplamente atingido, F - Plenamente atingido)
A.13.2.1 – Políticas e procedimentos de transferência de informação (1 de 2)	0	Incompleto	P – Parcialmente atingido
A.13.2.1 – Políticas e procedimentos de transferência de informação (2 de 2)	0	Incompleto	P – Parcialmente atingido
A.13.2.2 – Acordos sobre transferência de informação	0	Não implementado	N – Não atingido
A.13.2.3 – Mensagens eletrónicas	0	Incompleto	P – Parcialmente atingido
A.13.2.4 – Acordos de confidencialidade e de não divulgação	0	Não implementado	N – Não atingido
A.16.1.1 – Responsabilidades e procedimentos (1 de 2)	0	Incompleto	P – Parcialmente atingido
A.16.1.1 – Responsabilidades e procedimentos (2 de 2)	0	Não implementado	N – Não atingido
A.16.1.2 – Reportar eventos de segurança da informação	0	Não implementado	N – Não atingido
A.16.1.3 – Reportar pontos fracos de segurança da informação	0	Incompleto	P – Parcialmente atingido
A.16.1.4 – Avaliação e decisão sobre eventos de segurança da informação (1 de 2)	0	Incompleto	P – Parcialmente atingido
A.16.1.4 – Avaliação e decisão sobre eventos de segurança da informação (2 de 2)	0	Incompleto	P – Parcialmente atingido
A.16.1.5 – Resposta a incidentes de segurança da informação	0	Incompleto	P – Parcialmente atingido

Anexo XIV - Resultados (aplicação do Modelo de Capacidade de Processos COBIT 5)

Controlo	Nível (0 a 5)	Capacidade do Processo (0 – Incompleto/Não implementado, 1 - Executado, 2 - Gerido, 3 - Estabelecido, 4 - Previsível, 5 - Otimizado)	Escala (N - Não atingido, P - Parcialmente atingido, L - Amplamente atingido, F - Plenamente atingido)
A.16.1.6 – Aprender com os incidentes de segurança da informação (1 de 3)	0	Incompleto	P – Parcialmente atingido
A.16.1.6 – Aprender com os incidentes de segurança da informação (2 de 3)	0	Incompleto	P – Parcialmente atingido
A.16.1.6 – Aprender com os incidentes de segurança da informação (3 de3)	0	Incompleto	P – Parcialmente atingido
A.16.1.7 – Recolha de evidências	0	Incompleto	P – Parcialmente atingido

A Nossa Universidade

Colégio dos Jesuítas
Rua dos Ferreiros - 9000-082, Funchal

Tel: +351 291 209400
Fax: +351 291 209410
Email: gabinetedareitoria@uma.pt