Requisitos e recomendações para o desenvolvimento e operação de um SGSI – Abordagem com ISO 27001/27002

Instituto Politécnico de Leiria – Escola Superior de Tecnologia e Gestão

Gonçalo Miguel Conceição Vicente, 2210510

***Resumo*— O presento trabalho tem como âmbito a abordagem de requisitos e recomendações para o desenvolvimento e operação de um Sistema de Gestão da Segurança da Informação (SGSI), de acordo com os *international standards* ISO/IEC 27001 e ISO/IEC 27002.**

Este documento divide-se em 11 diferentes capítulos. Inicialmente é realizada uma introdução explicando sucintamente quem foram os criadores da duas ISO que compõem este trabalho e o que cada uma aborda. Seguidamente, é explicado o que é um Sistema de Gestão da Segurança da Informação. No terceiro capítulo é explicada a ISO 27001, quais os seus requisitos e controlos. No capítulo 4 são enunciados e explicados todos os requisitos da presente ISO. No cinto, sexto e sétimo capítulos é explicada a ISO 27002, os seus objetivos e o seu conteúdo. No capítulo 8, é explicado como se implementa um SGSI. No nono capítulo, é explicado no que consiste a certificação ISO 27001, nomeadamente os seus benefícios para a organização, clientes e fornecedores, o tempo de demora da certificação e certificadores reconhecidos em Portugal. No décimo capítulo é apresentada a importância da ISO 27001 no contexto da cibersegurança. Por fim, no capítulo 11, é feita a conclusão do trabalho.

***Index Terms*—Certificação, Cibersegurança, ISO/IEC 27001, ISO/IEC 27002, SGSI**

I. INTRODUÇÃO

AO longo do presente documento, irão ser abordados requisitos e recomendações para o desenvolvimento e operação de um SGSI, de acordo com as ISO 27001/27002.

A norma ISO/IEC 27001:2013 *Information technology – Security techniques – Information security management systems - Requirements* [1] resultara da colaboração entre os comités técnicos da ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*). Com esta ISO foi publicado um *standard* que fornece um modelo para estabelecer, implementar, operar, monitorizar, rever e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

A ISO/IEC 27002 *Information tecnology - Security techniques - Code of practise for information security controls* [2] é um código de melhores práticas para apoiar a implantação de um Sistema de Gestão da Segurança da Informação, nas organizações. Com o fornecimento de um conjunto completo de implementações, esta norma internacional descreve como os controlos podem ser estabelecidos para auxiliar a aplicação de um Sistema de Gestão da Segurança da Informação.

II. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO - SGSI

Ao longo dos últimos anos, e principalmente desde que se tem verificado a uma maior informatização de diversas organizações, os dados pertencentes a estas podem estar mais fáceis de aceder para pessoas mal-intencionadas. Assim, é necessário garantir aos clientes que as informações deles estão seguras. [3]

Assim, um SGSI é um conjunto de controlos que uma organização visa a implementar de forma a proteger os seus ativos, uma vez que é reduzida a possibilidade de indivíduos mal-intencionados conseguirem penetrar no seu sistema.

Desta forma, a aplicação de um sistema de processos dentro de uma organização, juntamente com a identificação e interação desses processos e a sua gestão pode ser referida como uma abordagem de processo.

A. Abordagem de processo

De acordo com a norma ISO/IEC 27001:2005 a abordagem de processo para um SGSI incentiva aos utilizadores a importância da compreensão de quais são os requisitos e qual a necessidade de estabelecer políticas e objetivos para a segurança da informação; implementar controlos de forma a gerir os riscos da segurança da informação de acordo com as necessidades da organização em questão; monitorizar e melhorar de forma continua o desempenho do SGSI.

Esta norma utiliza o modelo “Plan-Do-Check-Act” (PDCA) (Figura *1*) de forma a rever os procedimentos e a ajustando-os assim que haja necessidade.

Figura 1 - Modelo "Plan-Do-Check-Act"

III. ISO 27001

A ISO 27001 é o padrão e referência internacional para a segurança da informação.

Assim a adoção desta norma serva para que as organizações adotem um modelo adequado para o estabelecimento, implementação, operação, monitorização, revisão e gestão de um SGSI.

A ISO 27001, divide-se em duas componentes. Na primeira componente, estão definidas as regras e os requisitos de cumprimento da norma (Figura *2*); a segunda componente, o Anexo A, apresenta um conjunto de controlos que devem ser adotados pelas organizações (Figura *3*).

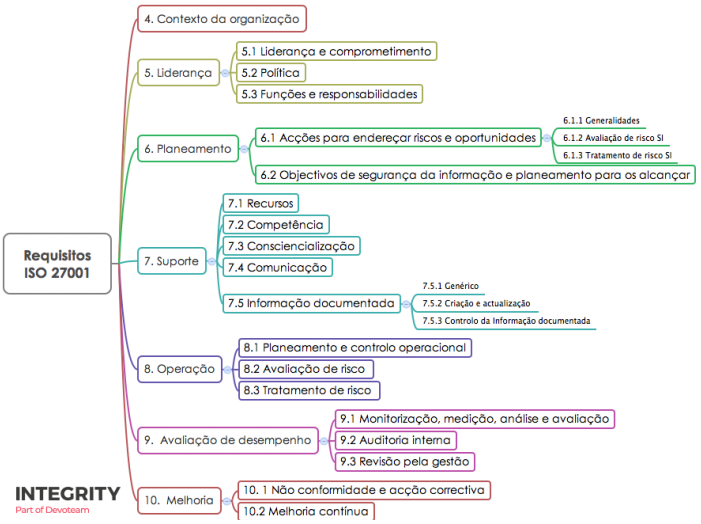

Figura 2 – Requisitos ISO 27001

Fonte: Integrity

Figura 3 – Controlos ISO 27001

Fonte: Integrity

IV. ISO/IEC 27001:2013 – Requisitos

Se uma organização pretender estar em conformidade com a ISO/IEC 27001:2013, é necessário que implemente um conjunto de requisitos independentemente das suas necessidades. Esses requisitos encontram-se definidos nas clausulas 4 a 10 da norma e caso não estejam aplicados, a organização não poderá afirmar que está em conformidade com o *International Standard* definido.

A. *Cláusula 4 – Contexto da organização*

Nesta cláusula são definidos os requisitos para compreender a organização e o seu contexto, entender as necessidades e expetativas das partes interessadas, o âmbito do SGSI bem como o objetivo de um SGSI.

De forma a compreender a organização e o seu contexto, esta deve determinar quais as questões externas e internas que são relevantes para o seu propósito e que afetam a sua capacidade para alcançar o resultado pretendido pelo seu SGSI.

Para ser possível entender as necessidades e expetativas das partes interessadas, a organização deve determinar quais os requisitos relevantes das partes interessadas para a segurança da informação.

De forma a entender o âmbito do SGSI, a organização deve determinar os limites de aplicabilidade do SGSI, devendo considerar as questões internas e externas, os requisitos e as atividades realizadas por si bem como por outras organizações.

A organização deve estabelecer, implementar, manter e melhorar um SGSI seguindo os requisitos do *Standard Internacional*.

B. *Cláusula 5 – Liderança*

Nesta cláusula são definidas responsabilidades, autoridades e compromissos da liderança da organização e políticas de segurança da informação.

A administração da organização deve demonstrar liderança e compromisso em relação o SGSI. Para tal, devem garantir que a política e os objetivos de segurança da informação estejam estabelecidos e sejam compatíveis com a direção estratégica da organização, garantindo a integração dos requisitos do SGSI nos processos desta.

É importante, também, que a administração disponibilize recursos necessários para o SGSI de forma que este atinja os resultados pretendidos, promovendo sempre uma melhoria contínua.

Relativamente à política de segurança da informação esta deve estar documentada e disponível para as partes interessadas e deve ser comunicada para dentro da organização. Além disso, deve ser apropriada para o propósito em que se insere a organização, incluindo objetivos de segurança da informação bem como um compromisso de melhoria continua do SGSI.

Existe ainda a necessidade de que a administração garanta que as responsabilidades e autoridades para funções relevantes no âmbito da segurança da informação sejam atribuídas e comunicadas, garantido que o SGSI esteja em conformidade com o *International Standard*.

*C. **Cláusula 6 – Planeamento***

Na cláusula 6 são abordados riscos e oportunidades. Ao planear o SGSI, a organização deve definir e aplicar um processo de avaliação de risco da segurança da informação, devendo ter em conta as questão e requisitos bem como determinar os riscos e as oportunidades que necessitam de ser abordadas. A organização, deve ainda, aplicar um plano de tratamento de risco da segurança da informação e definição de objetivos tendo em conta funções e níveis.

Aquando do planeamento do Sistema de Gestão de Segurança da Informação, a organização deve ter em conta as questões e requisitos bem como os riscos e oportunidades que necessitam de ser abordados. De forma a garantir que se pode obter o resultado pretendido, deve-se prevenir ou reduzir efeitos indesejáveis melhorando continuamente o SGSI. Assim, deve-se planear ações para lidar com riscos e oportunidades.

A organização deve definir e aplicar um processo para avaliação do risco de segurança da informação que estabeleça e mantenha critérios de risco de segurança da informação e que garanta que as avaliações de risco produzem resultados consistentes, válidos e comparáveis. É, também, importante identificar riscos da segurança da informação e quais as consequências caso esses riscos ocorressem.

A organização precisa de definir um plano de tratamento de risco da segurança da informação de forma a selecionar opções de tratamento apropriadas tendo em conta os resultados da avaliação de risco, abordada acima. É necessário produzir uma declaração de aplicabilidade que contenha quais e porquê os controlos necessários, se estes se encontram implementados ou não e qual a justificação, para o caso de não se encontrarem implementados.

Por fim, devem ser estabelecidos objetivos de segurança da informação em funções e níveis relevantes pela organização. Os objetivos e segurança devem estar em concordância com a política de segurança da informação, devendo ser comunicado e atualizado conforme apropriado. De forma a planear como atingir os objetivos de segurança da informação, deve-se responder às questões: O que deve ser feito? Quais os recursos que são necessários? Quem será o responsável? Quando será completado? Como serão avaliados os resultados? Além disto, devem estar documentas informações sobre os objetivos da segurança da informação.

*D. **Cláusula 7 – Suporte***

Nesta cláusula é referido que a organização deve determinar e fornecer os recursos necessários para o estabelecimento, implementação, manutenção e melhoria do SGSI. É realçado que a organização deve determinar que os trabalhadores devem ter a competência necessária e, quando possível, tomar medidas de forma a adquirem a competência necessária.

As pessoas que trabalham sob o controlo da organização devem estar cientes da política de segurança da informação sendo importante a sua contribuição para a eficácia do SGSI, caso contrário pode haver implicações na eficácia do SGSI.

Por fim, nesta cláusula é referido que o SGSI deve incluir informações documentadas pelo *International Standard*, sendo documentadas informações que a organização considere necessárias para a eficácia do SGSI, podendo variar a sua dimensão consoante o tamanho e o tipo de atividades praticadas; a complexidade dos processos e as interações e a competência das pessoas. Todas as informações documentas devem ser devidamente protegidas, porém devem estar disponíveis para quando for necessário o seu uso.

*E. **Cláusula 8 – Operação***

Na cláusula 8 são definidos os planos e controlos operacionais, a avaliação e tratamento de risco da segurança da informação.

Relativamente aos planos e controlos operacionais, a organização deve planear, implementar e controlar os processos necessários para cumprir os requisitos de segurança da informação, devendo manter as informações documentadas para ter confiança de que os processos foram realizados conforme planeado.

No que diz respeito à avaliação e tratamento de risco da segurança da informação, a organização deve realizar avaliações de risco da segurança da informação em intervalos de tempo definidos ou quando ocorrem mudanças significativas sendo necessário fazer uma nova avaliação devendo, então, implementar um plano para o seu tratamento.

Tanto os resultados da avaliação como do tratamento de risco da segurança da informação devem estar documentos.

*F. **Cláusula 9 – Avaliação de desempenho***

Na cláusula 9 são definidos os requisitos para a monitorização, medição, análise, avaliação, auditoria e revisão pela administração da organização.

No que diz respeito à monitorização, medição, análise e avaliação, a organização deve avaliar o desempenho da segurança da informação e a eficácia do SGSI, como por exemplo saber quando e o que precisa de ser monitorizado e medido, incluindo os processos e controlos de segurança da informação bem como quem deve analisar e avaliar esses resultados.

Relativamente à auditoria interna, a organização deve realizar auditorias internas em intervalos de tempo planeados de forma a fornecer informações sobre se o SGSI está efetivamente implementando e se encontra conforme os próprios requisitos da organização e do *Internation Standard*. Devem ainda ser definidos critérios para cada auditoria bem como selecionar auditores de forma a garantir objetividade e imparcialidade. Por fim, o programa de auditoria e os resultados devem ser documentados.

No âmbito da revisão, a administração da organização deve rever o SGSI em intervalos de tempo definidos de forma a garantir que continuam adequados e eficazes. Para tal, a gestão da organização deve ter em conta o resultado de análises anteriores; mudanças, tanto internas como externas e que possam afetar o SGSI; resultados da avaliação de risco e o estado do plano de tratamento de risco e oportunidades de melhoria contínua.

*G. **Cláusula 10 – Melhorias***

Ao longo desta cláusula são definidos os requisitos para não conformidades, ações corretivas e melhorias continuas.

Assim, quando ocorre um não conformidade, a organização deve tomar medidas para controlá-la e corrigi-la, sendo necessário avaliar a necessidade de ações para eliminar as causas da não conformidade, a fim de que ela não se repita. Poderá existir a necessidade de fazer alterações no SGSI, devendo estas alterações ser adequadas aos efeitos das não conformidades encontradas.

A organização deve documentar estas informações, nomeadamente a natureza das não conformidades encontradas, bem como o resultado de qualquer ação corretiva.

Além disso, a organização deve melhorar continuamente a idoneidade, adequação e eficácia do SGSI.

V. ISO/IEC 27002:2013

No ano de 1995, duas organizações internacionais (ISO – *The International Organization for Standardization e* IEC – *International Electrotechnical Commission*) construíram um conjunto de normas que fortaleceram as diretrizes relacionadas com a Segurança da Informação. Assim, surgiu a família ISO/IEC 27000, da qual faz parte a ISO/IEC 27001, abordada acima, e a ISO/IEC 27002 que será abordada neste capítulo, entre outras normas que não são relevantes para o contexto do presente trabalho. [4]

A ISO/IEC 27002 é um código de melhores práticas para apoiar a implantação de um Sistema de Gestão da Segurança da Informação, nas organizações. Com o fornecimento de um conjunto completo de implementações, esta norma internacional descreve como os controlos podem ser estabelecidos para auxiliar a aplicação de um SGSI. De forma a estabelecer estes controlos, é necessária uma avaliação de riscos dos ativos mais importantes da empresa. [5]

É recomendado que esta norma seja utilizada em conjunto com a ISO 27001, mas também pode ser consultada de forma independente para a adoção de boas práticas.

VI. ISO 27002:2013 – Objetivos

A ISO 27002 tem como principal objetivo estabelecer diretrizes e princípios de forma a iniciar, implementar, manter e melhorar a gestão da segurança da informação numa organização (independentemente da dimensão e da área em que opere).

VII. ISO 27002:2013 – Conteúdo

A ISO 27002:2013 divide-se em várias secções como é possível visualizar na Figura *4*. De seguida, serão abordadas as diferentes secções desta norma.

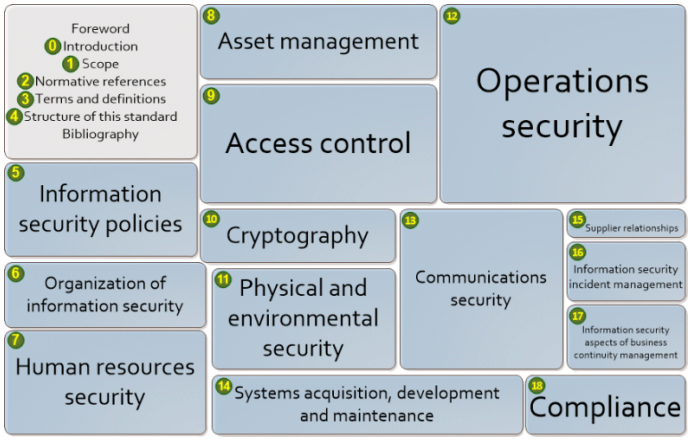

Figura 4 - Capítulos ISO 27002:2013

Fonte: SecAware

A. *Secção 0 – Introdução*

Nesta secção é descrito o contexto histórico em que se a ISO se insere, sendo mencionados requisitos de segurança da informação, controlos, o desenvolvimento de diretrizes próprias, considerações acerca do ciclo de vida bem como normas selecionadas.

Ao longo desta secção, existem três requisitos para a segurança da informação: a partir da análise de riscos é necessário ter em conta os objetivos e estratégias globais de negócio da organização, sendo identificadas as ameaças aos ativos, as vulnerabilidades e realizada uma estimativa da probabilidade da ocorrência de ameaças e o seu potencial impacto no negócio; a legislação, os estatutos, a regulamentação e as cláusulas contratuais que a organização, os seus parceiros de negócios, contratados e fornecedores de serviços tem que obedecer; os conjuntos particulares de princípios, objetivos e requisitos do negócio para manuseamento, processamento, armazenamento, comunicação e arquivo da informação que uma organização necessita de desenvolver de forma a apoiar as suas operações.

Relativamente à seleção de controlos, estes dependem das decisões da organização, baseadas nos critérios para aceitação de risco e nas opções de tratamento do risco.

Em relação ao desenvolvimento de diretrizes próprias, esta norma pode ser considerada como um ponto de partida. Nem todos os controlos e diretrizes podem ser aplicados bem como pode existir a possibilidade de adicionar controlos adicionais que não se encontram na ISO 27002.

No que diz respeito às considerações acerca do ciclo de vida, as informações têm um clico de vida passando pela sua criação e origem, armazenamento, processamento, uso e transmissão até à sua possível destruição, variando o seu valor e riscos durante esses processos. Contudo, a segurança da informação é importante em algumas etapas. Um processo semelhante acontece com os sistemas de informação, devendo

a segurança da informação ser considerada em cada ciclo.

B. Secção 1 – Âmbito

A ISO 27002 fornece diretrizes para boas práticas de gestão de segurança da informação bem como normas de segurança da informação para organizações, como a seleção, implementação e gestão de controlos tendo em consideração os ambientes de risco da segurança da informação, da organização.

Esta norma é projetada de forma a ser usada por organizações que pretendem: selecionar controlos dentro do processo de implementação de um SGSI baseado na ISO/IEC 27001; implementar controlos de segurança mundialmente reconhecidos; desenvolver os seus próprios princípios de gestão da segurança da informação.

C. Secção 2 – Referências Normativas

O único documento indispensável para a aplicação desta norma é a ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

D. Secção 3 – Termos e definições

Ao longo deste documento, são aplicados os termos e definições da ISO/IEC 27000.

E. Secção 4 – Estrutura

Esta ISO contém 14 secções de controlos de segurança da informação, 35 objetivos e 114 controlos.

Em cada secção são definidos controlos de segurança da informação e cada uma contém um ou mais objetivos de controlo, sendo que a ordem pela qual se encontram não é representativa do seu grau de importância, uma vez que dependendo das circunstâncias, os controlos de qualquer uma das secções podem ser importantes. Assim, convém que cada organização implemente esta norma, identificando quais são os controlos que se aplicam, quão importante são e qual é a aplicação nos processos individuais da organização.

Relativamente à categoria de controlos, cada secção principal contém: um objetivo de controlo declarando o que se pretende alcançar; um ou mais controlos que podem ser aplicados para se alcançar o objetivo de controlo.

São ainda apresentadas informações mais detalhadas de forma a apoiar a implementação do controlo e alcançar o seu objetivo. Deve-se ter em conta que, as diretrizes podem não ser totalmente adequadas ou suficientes em todas as situações, podendo existir a possibilidade de não preencherem completamente os requisitos de controlo específicos da organização.

F. Secção 5 – Políticas de segurança da informação

Relativamente às políticas de segurança da informação, devem-se implementar mecanismos de controlo que sejam aprovados pela direção, publicados e comunicados a todos os funcionários bem como a eventuais partes externas relevantes. É importante que a liderança da organização defina uma política de segurança da informação de forma a estabelecer a abordagem da organização parar gerir os objetivos de segurança da informação.

Existe ainda a necessidade de políticas internas de segurança da informação, porém varia consoante as organizações. Normalmente são uteis em organizações maiores e mais complexas onde quem define e aprova os controlos são pessoas diferentes de quem os implementa.

É importante que exista uma análise critica das políticas para a segurança da informação, em intervalos de tempo previamente programados ou quando existe uma mudança significativa de forma a assegurar a sua contínua pertinência, adequação e eficácia.

G. Secção 6 – Organização da segurança da informação

Deve-se estabelecer uma estrutura de gestão de forma a iniciar e controlar a implementação da segurança da informação dentro da organização.

Desta forma, devem ser atribuídas e definidas, em conformidade com as políticas, responsabilidades para a segurança da informação. Convém que funcionários que tenham responsabilidades pela segurança da informação deleguem para outros utilizadores as tarefas de segurança da informação, porém continuam a ser os responsáveis por verificar se as tarefas delegadas estão a ser executadas corretamente. Algumas empresas optam por atribuir a um gestor de segurança da informação a responsabilidade pelo desenvolvimento, implementação e identificação de controlos, ficando a responsabilidade por pesquisar e implementar os controlos em gestores individuais.

A segregação de funções é importante, uma vez que assim são reduzidas oportunidades de modificação não autorizadas ou não intencionais. Convém que existam cuidados de forma a impedir que uma única pessoa possa ter acesso, modificar ou utilizar ativos sem a devida autorização. Assim, a segregação de funções é um método para reduzir o risco de mau uso, acidental ou deliberado dos ativos de uma organização.

Os contactos com as autoridades, grupos especiais, associações de profissionais e outros fóruns especializados são importantes e para tal, deve haver procedimentos implementados de forma a especificar, quando e quem deve ser contactado e como identificar os incidentes de segurança da informação.

Um outro requisito importante é que a segurança da informação também seja tida em conta na gestão dos projetos, independentemente do tipo de projeto.

Deve-se garantir a segurança da informação no trabalho remoto e no uso de dispositivos móveis. Assim, existe a necessidade de uma política e medidas que sejam adotadas para gerir os riscos do uso de dispositivos móveis. Relativamente ao trabalho remoto, é importante a existência de políticas e medidas que sejam implementadas de forma a proteger as informações que podem ser obtidas, processadas ou armazenadas em locais de trabalho remoto.

H. Secção 7 – Segurança dos recursos humanos

De forma que exista segurança dos recursos humanos, é importante que os funcionários e partes externas entendem as

suas responsabilidades e que estejam em conformidade com os papéis para os quais foram selecionados.

Durante um período de seleção torna-se importante a confirmação do que o candidato afirma possuir, por exemplo se as informações do *curriculum vitae* e as qualificações académicas são reais. Também é relevante, quando um individuo é contratado para desempenhar papeis de segurança da informação que tenha a competência necessária para essas atividades e que se sinta suficientemente confiável para as desempenhar. Além disso, nos termos e condições do contrato devem estar definidas responsabilidades para a segurança da informação.

Durante a contratação, deve-se assegurar que os funcionários e partes externas estão conscientes e cumprem as responsabilidades pela segurança da informação. É fundamental que a direção demonstre o seu apoio às políticas, procedimentos e controlos e aja de forma exemplar, uma vez que se os funcionários e fornecedores não tiverem consciência das suas responsabilidades em segurança da informação podem causar danos consideráveis a uma organização. Quando existir uma violação da segurança da informação deve ser implantado e comunicado um processo disciplinar formal, de forma a tomar ações contra o funcionário que cometeu essa violação.

I. Secção 8 – Gestão de ativos

De forma proteger os ativos da organização é necessário identificar quem são e quais as suas responsabilidades. Para tal, deve-se estruturar e manter um inventário dos ativos e saber quem é o seu proprietário. Devem existir regras de forma que os funcionários ou partes externas tenham consciência dos requisitos de segurança da informação dos ativos da organização. Quando um funcionário ou parte externa cessar funções com a organização, deve devolver todos os ativos da organização que possam estar em sua posse.

De forma a garantir que a informação recebe um nível apropriado de proteção, esta deve estar classificada de acordo com o valor, requisitos legais, sensibilidade e criticidade de forma a evitar a sua modificação ou divulgação não autorizada. Para tal, deve estar desenvolvido e implementado um conjunto de procedimentos para rotular e tratar a informação, de acordo com o esquema de classificação adotado pela organização.

Relativamente aos media de uma organização, esta deve ter procedimentos implementados para a sua gestão e eliminação. Assim, quando os media não forem mais necessários, devem ser descartados através de procedimentos formais. Por outro lado, os media que contém informações devem ser protegidos contra o acesso não autorizado, uso impróprio ou corrupção, durante o transporte, entre outros.

J. Secção 9 – Controlo de acesso

A organização deve estabelecer, documentar e analisar uma política de controlo de acesso, baseada nos requisitos de segurança da informação e dos negócios. Neste sentido, os utilizadores da organização apenas devem receber acessos a redes e serviços para o qual tenham sido autorizados a utilizar. Para isso, deve ser necessário autenticação para os serviços bem como o seu monitoramento.

Existe a necessidade de implementar um processo formal para o registo ou cancelamento de utilizadores, de forma a permitir a atribuição de diferentes direitos de acessos. Assim, é possível conceder ou revogar os acessos do utilizador para todos os papéis de utilizadores existentes no diversos sistemas e serviços.

De forma periódica, devem ser analisados cuidadosamente os direitos de acessos dos utilizadores para garantir que todos tem as permissões que devem ter e não mais do que isso. Aquando do termino ou mudança de funções, todos os direitos de utilizadores devem ser retirados/ajustados para a nova função que irá ser desempenhada.

Relativamente ao processo de autenticação, os utilizadores devem ser responsáveis por proteger as suas informações. Para tal, os funcionários devem ser orientados a seguir as práticas da organização, contudo os sistemas de gestão de *passwords* devem ser iterativos e devem assegurar que o utilizador utiliza *passwords* de qualidade.

Tanto o uso de programas que requerem privilégios especiais bem como o acesso ao código fonte devem ser restritos e estritamente controlados.

K. Secção 10 – Criptografia

A organização deve assegurar o uso adequado de criptografia de forma a proteger a confidencialidade, autenticidade e integridade da informação. Assim, deve ser desenvolvido e implementado uma política para o uso de controlos criptográficos de forma a proteger a informação, devendo ser tido em conta as leis ou regulamentações e restrições nacionais aplicadas ao uso de técnicas criptográficas.

Uma política sobre o uso, proteção e ciclo de vida das chaves criptográficas deve ser desenvolvida e implementada. Esta política deve ter conta a gestão, armazenamento, arquivo, recuperação, distribuição, retirada e destruição das chaves.

L. Secção 11 – Segurança física e do ambiente

A organização deve implementar mediadas de forma a prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações da organização.

Neste sentido, convém que sejam definidos e usados perímetros de segurança de forma a proteger as áreas onde se encontram as informações mais críticas da empresa. Para tal, pode-se obter uma proteção com a criação de uma ou mais barreiras físicas. O uso de controlos de entrada também é crucial para garantir que apenas pessoas autorizadas tem acesso ao seu interior.

Durante este processo, também deve ser tido em conta uma proteção contra ameaças ambientais, por exemplo, desastres naturais e acidentes. Assim, deve-se obter orientações de especialistas sobre como evitar danos provocados por fogo, inundações, terramotos, explosões, manifestações civis, entre outras formas de desastres naturais.

De forma a evitar acessos não autorizados, as áreas de entrega e carregamento devem ser controladas e, se possível, ficarem isoladas das instalações onde se encontram informações importantes que não devem ser acedidas sem que tenham autorização para tal.

Os equipamentos também são um ativo importante para uma empresa, nesse sentido devem ser protegidos de forma a evitar perdas, danos, furtos ou comprometimento das operações da organização bem como a organização deve assegurar uma manutenção dos mesmos. Assim, convém que sejam colocados no local ou protegidos para reduzir os riscos. Estes, também devem estar protegidos contra falta de energia elétrica e outras interrupções que possam acontecer.

Além dos equipamentos, também os cabos de energia e telecomunicações que transportam dados ou permitem acesso a serviços de informações devem estar protegidos contra intercetações, interferência ou danos.

Nenhum equipamento deve ser retirado sem autorização prévia e para os equipamentos que se encontram fora da organização, devem ser tomadas medidas de segurança, tendo em conta os riscos associados a estarem a trabalhar fora da empresa.

Relativamente à reutilização de equipamentos, em especial discos de armazenamento, devem ser examinados de forma a garantir que todos os dados importantes e softwares licenciados encontram-se removidos antes do equipamento ser descartado.

M. *Secção 12 – Segurança nas operações*

A organização deve garantir que os procedimentos de operações se encontram documentados e disponibilizados a todos os utilizadores que necessitem deles. Nesse documento, devem estar procedimentos de iniciar e desligar os computadores, geração de cópias de segurança, manutenção de equipamentos, tratamento de medias, segurança e gestão do tratamento das correspondências e das salas de computadores.

Numa organização, mudanças nos processos de negócio, recursos de processamento da informação e nos sistemas que afetam a segurança da informação devem ser feitas de forma controlada.

De forma a reduzir riscos de acessos ou modificações não autorizadas no ambiente de produção, os ambientes de desenvolvimento, teste e produção devem ser separados. De igual forma, devem ser implementados controlos de deteção, prevenção e recuperação para proteger a organização contra ataques maliciosos, sendo para isso importante a consciencialização do funcionário.

A organização deve implementar medidas para que existam regularmente cópias de segurança das informações, softwares e das imagens do sistema.

Numa empresa, os registos de *log* [6] (eventos das atividades dos utilizadores e falhas) são bastantes importantes, devendo ser produzidos, mantidos e analisados cuidadosamente. Devido à sua importância, devem estar devidamente protegidos contra acessos não autorizados e adulterações.

Manter a data e hora dos equipamentos sincronizada, é bastante importante. Para tal, deve-se sincronizar todos com uma única fonte de tempo precisa, uma vez que a exatidão da data e hora pode vir a ser relevante em análises futuras.

Na instalação de software nos sistemas operativos, devem ser implementados procedimentos para controlar essa instalação, utilizando regras com critérios definidos. Manter o *software* atualizado também pode ser crucial, uma vez que *software* desatualizado pode ser uma porta de entrada para agentes maliciosos bem como aplicar pacotes de correção de *software* para reduzir vulnerabilidades de segurança da informação.

Relativamente à gestão de vulnerabilidades técnicas, convém que essas informações sejam obtidas rapidamente, sendo a exposição da organização avaliada e tomadas medidas apropriadas para lidar com os riscos associados.

Por fim, controlos de auditoria aos sistemas de informação devem ser devidamente planeados e acordados para minimizar o tempo de auditoria no processo de negócio da organização.

N. *Secção 13 – Segurança nas comunicações*

Numa organização é importante que a rede seja gerida e controlada de forma a proteger as informações nos sistemas e aplicações.

De forma a proteger a segurança dos serviços de rede, os mecanismos de segurança, níveis de serviço e requisitos de gestão de todos os serviços de redes, devem estar identificados e incluídos nos acordos de serviços, tanto a nível interno como externo. A segregação de redes também deve ser adotada, dividindo a rede em diferentes redes físicas ou utilizando redes lógicas, recorrendo, por exemplo, ao uso de *VPN* [6].

No que diz respeito à transferência de informação, deve-se manter a segurança da informação transferida dentro da organização. Para tal, devem-se aplicar políticas, procedimentos e controlos de transferências formais de forma a proteger a transferência das informações. Para transferências de informações entre a organização e partes externas, deve ser estabelecido acordos de forma a garantir a segurança da informação.

Relativamente a mensagens eletrónicas, por exemplo *emails*, *Eletronic Data Interchange* e redes sociais, estas devem estar devidamente protegidas.

O. *Secção 14 – Aquisição, desenvolvimento e manutenção de sistemas*

Aquando da especificação de requisitos para novos sistemas de informação ou melhorias em sistemas já existentes, devem estar incluídos requisitos relacionados com a segurança da informação.

Para tal, convém que as regras para o desenvolvimento de sistemas e *software* estejam estabelecidas e aplicadas para os desenvolvimentos da organização. Assim, o desenvolvimento seguro é um requisito para construir um serviço, uma arquitetura, um software e um sistema seguro.

De forma a evitar problemas como mudanças em software, deve-se fazer testes num ambiente controlado em laboratório, para que eventuais problemas não se estendam para a restante organização.

Por vezes, existe a necessidade de modificações em pacotes de *software* de fornecedores. Essas mudanças são desencorajadas e estão limitadas apenas a mudanças necessárias. Porém, tal nunca deve acontecer sem obtenção de consentimento por parte do fornecedor do *software*.

De forma a projetar sistemas seguros, devem ser estabelecidos, documentados, mantidos e aplicados para qualquer implementação, devendo ser feito num ambiente de desenvolvimento devidamente protegido. Quando são sistemas desenvolvidos por terceiros, a organização deve supervisionar

e monitorizar todas as atividades de desenvolvimento, sendo realizados testes de funcionalidades de segurança durante o desenvolvimento do sistema.

Os dados utilizados para efeitos de teste devem ser dados selecionados com cuidado, protegidos e controlados, evitando assim a utilização de base de dados que se encontrem em modo de produção.

P. Secção 15 – Relação com fornecedores

Na política de segurança da informação, na relação com cada fornecedor que possa aceder à organização, os requisitos de segurança da informação para mitigar os riscos que se encontram relacionados com o acesso de terceiros aos ativos da organização devem estar acordados e documentados.

A entrega de serviços por parte de fornecedores deve ser monitorizada e analisada pela organização em intervalos regulares de forma a monitorizar se os acordos se encontram a ser cumpridos.

Mudanças nos acordos com os fornecedores devem ser geridas tendo em conta o grau de importância das informações da organização, dos sistemas e processos envolvidos e uma reavaliação de riscos. Essas alterações devem incluir manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controlos existentes.

Q. Secção 16 – Gestão de incidentes de segurança da informação

Estabelecer responsabilidades e procedimentos de gestão são importantes de forma a assegurar respostas rápidas e efetivas a incidentes de segurança da informação. Os objetos para a gestão de incidentes de segurança devem estar acordados com a direção da organização e que garantam que o responsável por fazer a gestão entenda as prioridades da empresa para gerir os incidentes da segurança da informação.

Todos os funcionários e partes externas devem ser alertados sobre a sua responsabilidade de notificar qualquer evento de segurança da informação o mais rápido possível, para tal pode haver a necessidade de instruir as pessoas a registar e notificar qualquer suspeita de fragilidade, por exemplo, quando existe um mau funcionamento ou um comportamento anômalo do sistema pode vir a ser um indicador de um ataque ou violação de segurança, portanto deve ser prontamente notificado.

Depois de haver um alerta por parte dos funcionários, os eventos reportados devem ser avaliados com o uso de uma escala de classificação de incidentes e eventos de segurança da informação, de forma a decidir se é ou não um incidente de segurança da informação. Assim, caso se classifique como um incidente, deve ser reportado para um ponto de contacto definido e outras pessoas relevantes na organização.

É importante que a organização defina e aplique procedimentos para a identificação, aquisição e preservação das informações, que podem servir como evidências para propósitos legais ou disciplinares.

R. Secção 17 – Aspetos da segurança da informação na gestão da continuidade do negócio

A organização deve avaliar se a continuidade da segurança da informação está contida dentro do processo de gestão da continuidade do negócio ou no processo de gestão de recuperação de desastre. Caso não esteja especificado, irá ser considerado que os requisitos de segurança da informação permanecem inalterados, ou seja, são os mesmos que existem numa situação normal.

A empresa deve estabelecer, documentar, implementar e manter processos, procedimentos e controlos para assegurar a continuidade da segurança da informação durante uma situação adversa.

Em intervalos de tempo regulares, a organização deve verificar se os controlos estabelecidos e implementados para a continuidade da segurança da informação são válidos e eficazes em situações adversas.

De forma que verifiquem os requisitos de disponibilidade, os recursos de processamento da informação devem ser implementados com um nível de redundância suficiente.

S. Secção 18 – Conformidade

Os requisitos legais e contratuais devem estar explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização. Assim, devem ser implementados procedimentos adequados de forma a garantir a conformidade destes.

Os registos devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e dispensa não autorizada de acordo com os requisitos legais e contratuais do negócio.

A privacidade e proteção das informações de identificação pessoal devem ser garantidas conforme presente na legislação, bem como o uso de criptografia deve estar em conformidade com as leis vigentes.

A forma como a organização está a gerir a segurança da informação e a sua implementação deve ser analisado de forma independente, em intervalos definidos ou quando ocorrem mudanças significativas. Os gestores devem, também, analisar em intervalos de tempo definidos, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade com as normas e políticas de segurança.

VIII. Como implementar um SGSI

Após ser enunciado os requisitos gerais das ISO 27001 e 27002, é possível implementar um Sistema de Gestão de Segurança da Informação. A implementação de um SGSI é uma mais-valia para as empresas, uma vez que seguindo as recomendações das ISO, é possível garantir a segurança dos seus ativos, porém para se obter os benefícios totais de um SGSI deve ser estabelecida uma implementação completa.

Assim, de forma a implementar um SGSI, deve-se realizar uma identificação e avaliação de ativos, ou seja, quais os ativos que devem ser protegidos e qual é o seu valor para a organização, sendo o valor classificado com base nos requisitos legais, sensibilidade e criticidade das informações. A organização deve encontrar uma forma de proteger os ativos, mas ao mesmo tempo permitir que funcionários que necessitem

de aceder para realizar o seu trabalho o possam fazer adequadamente.

Após ser realizado a identificação e avaliação de ativos, existe a necessidade de efetuar uma avaliação de risco, que consiste em determinar como os ativos deverão ser protegidos com base na análise de ameaças e vulnerabilidades, impacto e como pode ser realizada a mitigação.

Nesse sentido, as organizações devem analisar as ameaças que cada um dos seus ativos pode sofrer, nomeadamente o seu uso por quem não está autorizado a fazê-lo, resultando em perdas ou danos e verificar quais estão mais vulneráveis às ameaças identificadas. Após estar definido as ameaças e vulnerabilidades, existe a necessidade de definir o impacto que as violações de segurança podem causar à organização e verificar quais são mais prejudiciais. Por fim, usando as políticas existentes num SGSI, deve-se definir métodos de forma a minimizar as ameaças e vulnerabilidades bem como o impacto que pode ter na vida da organização.

Depois de a organização ter realizado a identificação e avaliação dos ativos e a análise de risco, devem estabelecer políticas e procedimentos para compor o SGSI.

O seguimento das ISO 27001 e 27002 não é obrigatório caso a organização não pretenda obter uma certificação relacionada com os sistemas de gestão da segurança da informação. Contudo, uma certificação ISO 27001 representa um conjunto de benefícios tanto para a organização como para clientes e fornecedores.

IX. Certificação ISO 27001

A certificação ISO 27001 representa um conjunto de benefícios para empresas, clientes e fornecedores. Na Figura *6*, é possível visualizar um conjunto de benefícios, sendo que serão explicados mais pormenorizadamente nos próximos subcapítulos.

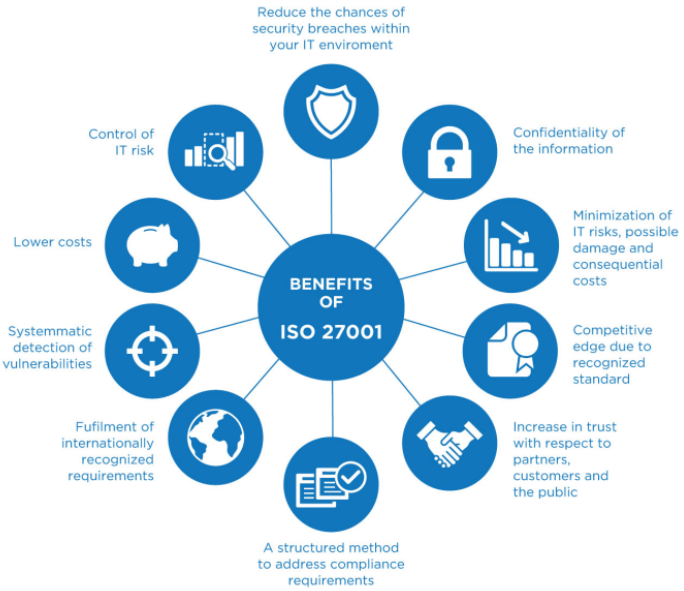

Figura 6 – Benefícios da ISO 27001

Fonte: Beliver Compilance

A. *Organização*

A adoção de práticas de gestão documentadas na ISO 27001 representa um conjunto de benefícios:

1. Demonstra preocupação da organização para com a segurança da informação;
2. Aumenta a segurança da informação e dos sistemas, nomeadamente em termos de confidencialidade, integridade e disponibilidade;
3. Aumenta os níveis de sensibilidade, participação e motivação dos funcionários para a segurança da informação;
4. Identifica de forma contínua ameaças e vulnerabilidades a que uma organização está sujeita;
5. Garantia de proteção dos sistemas em todo o ciclo de desenvolvimento;
6. Monitorização contínua das infraestruturas que suportam os sistemas.

B. *Clientes e fornecedores*

Os clientes e fornecedores de uma organização certificada com a ISO 27001, também obtêm benefícios, uma vez que essa organização garante um elevado nível com a proteção da informação e, assim, clientes e fornecedores sabem que a informação sobre a sua empresa será tratada com um elevado grau de segurança da informação, uma vez que existiu uma auditoria por uma empresa externa e confiável.

C. *Tempo de demora para a certificação*

De forma a preparar a certificação, é necessário a implementação e adoção de requisitos, políticas, procedimentos, controlos e práticas requeridas na ISO 27001. Contudo, o tempo de implementação varia de acordo com a realidade e dimensão de cada organização. Na Figura *5*, é possível visualizar um processo típico de certificação, onde poderá demorar entre 7 a 16 meses.

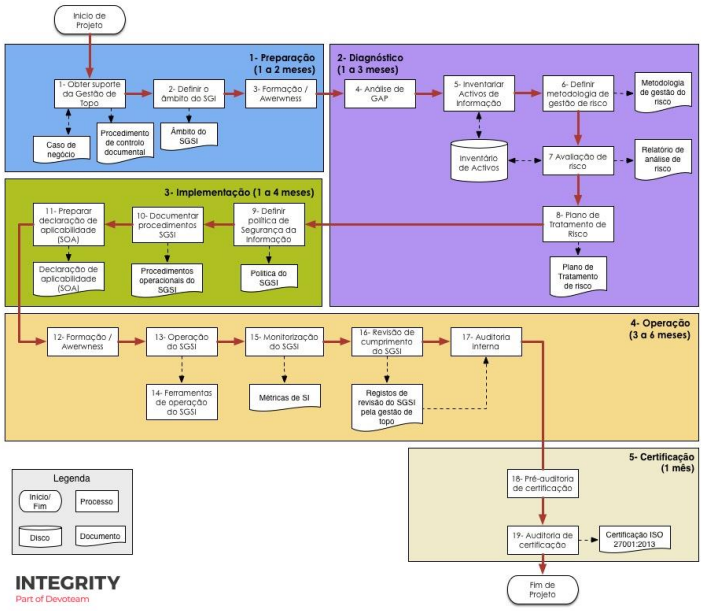

Figura 5 – Diagrama do processo de certificação

Fonte: Integrity

D. Certificadores

Em Portugal, a INTEGRITY [8] possuiu consultores formados e certificados com a ISO 27001 *Lead Auditors*, preparados para ajudar no ato de preparação, implementação e adoção de um SGSI com base na ISO.

De forma a certificar, existe a Associação Portuguesa de Certificação (APCER) [9], Serviços Internacionais de Certificação, Lda (SGS) [10] e Empresa Internacional de Certificação, S.A. (EIC) [11].

X. ISO 27001 e cibersegurança

A ISO 27001 apresenta um papel importante relativamente à cibersegurança. Através desta norma internacional, é possível existir uma deteção de vulnerabilidades e riscos a que os sistemas podem estar expostos bem como o cumprimento de diversos requisitos internacionais impostos em diferentes setores de atividade.

Esta ISO permite que aja uma garantia de confidencialidade, integridade e disponibilidade dos dados através da implementação de 114 medidas, fazendo com que a ISO 27001 seja um dos guias de segurança mais completos e eficazes.

Por fim, com a transformação digital de cada vez mais empresas e consequentemente o incremento dos recursos à Internet ou dispositivos de *cloud*, as empresas tem vindo a aumentar a sua proteção face a ciberataques. Ao contrário do que se pode pensar, não são apenas as grandes empresas os alvos dos atacantes, sendo as pequenas/médias empresas os alvos preferenciais uma vez que tem menor capacidade para se defenderem. [12]

XI. Conclusão

O valor da informação não é apenas o que está representado através de palavras, pode haver ideias de negócio por detrás de um documento furtado. Assim, a informação, processos, sistemas, redes e pessoas são ativos que tem valor para o negócio da organização e nesse sentido requer proteção contra vários riscos.

Enquanto os ativos são alvo de ameaças, tanto acidentais como propositadas, os processos, sistemas, redes e pessoas têm vulnerabilidades. Mudanças nos processos e sistemas de negócio podem criar novos riscos de segurança da informação.

Uma segurança da informação eficaz reduz riscos, protegendo a organização de ameaças e vulnerabilidades de forma a reduzir o impacto nos seus ativos.

Para se alcançar a segurança da informação é necessário seguir um conjunto de controlos, políticas, processos e procedimentos. Estes controlos ser estabelecidos, implementados, monitorizados, analisados e melhorados continuamente para garantir que a segurança da informação da organização se encontra eficaz.

Desta forma, as recomendações das ISO 27001 e 27002 ajudam a estabelecer um SGSI com controlos reconhecidos mundialmente.

Referências

[1] “ISO/IEC 27001:2013 – SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO,” [Online]. Available: www.sgs.pt. [Acedido em 25 10 2021].

[2] “ISO 27002: Boas práticas para gestão de segurança da informação,” [Online]. Available: ostec.blog. [Acedido em 25 10 2021].

[3] “ABNT- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação,” 2005. [Online].

[4] “O que é ISO 27001 e 27002?,” [Online]. Available: www.portalgsti.com.br. [Acedido em 25 10 2021].

[5] D. Kosutic, “Semelhanças e diferenças entre a ISO 27001 e a ISO 27002,” [Online]. Available: advisera.com. [Acedido em 25 10 2020].

[6] “ISO 27001 Sistema de Gestão de Segurança da Informação,” [Online]. Available: www.27001.pt. [Acedido em 30 10 2020].

[7] “ISO/IEC 27001,” [Online]. Available: www.apcergroup.com. [Acedido em 30 10 2021].

[8] “ISO/IEC 27001:2013 – SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO,” [Online]. Available: www.sgs.pt. [Acedido em 31 10 2021].

[9] “QUAL O PAPEL DA ISO 27001 NA CIBERSEGURANÇA?,” 20 10 2021. [Online]. Available: sgs.pt. [Acedido em 31 10 2021].

[10] “CERTIFICAÇÃO DE SEGURANÇA DA INFORMAÇÃO,” [Online]. Available: www.eic.pt.

[11] “O que é uma VPN e como funciona?,” [Online]. Available: www.kaspersky.com.br. [Acedido em 25 10 2021].

[12] “O que é um log?,” [Online]. Available: support.ankama.com. [Acedido em 29 10 2021].

[13] “ISO/IEC 27001:2017 - Information technology - Security techniques - Information security management systems - Requirements”. 31 3 2017.

[14] “ISO/IEC 27002:2013 Information tecnology - Security techniques - Code of practise for information security controls”. 31 3 2017.