Project Report

Cybersecurity & Next Generation Technologies and Services

Master in Computer Engineering Mobile Computing

O RGPD e a sua implementação através da utilização da família de normas ISO 27000

Tiago Alexandre Pinheiro Martins

2182716

Leiria, Janeiro de 2019

This page was inthetionally left blank

Resumo

A informação tem vindo a ser um dos ativos mais importantes para as empresas e organizações. Informações relativas a utilizadores são o tipo de informação mais rentável para empresas de publicidade personalizada e muitas companhias beneficiam da posse da informação dos utilizadores para vender a ditas empresas. De modo a combater esta exploração a dados pessoais, a união europeia começou a desenvolver uma regulamentação que protegesse os utilizadores. Com a introdução do RGPD em 25 de Maio de 2018, muitas empresas e organizações não sabiam bem que procedimentos tomar de forma a estar em conformidade com o regulamento. No regulamento para além dos utilizadores ganharem bastantes direitos, as organizações têm agora também que seguir vários princípios, sendo alguns deles referentes à segurança da informação que guardam acerca os seus utilizadores.

De modo a estar em conformidade e não receberem coimas, as organizações têm que garantir a segurança da informação que recolhem dos seus clientes / utilizadores.

As normas da família ISO 27000 focam-se na segurança da informação e são um bom guia para entrar em conformidade com estes princípios impostos pelo RGPD.

A ISO 27001 estabelece o conceito de um sistema de gestão de segurança de informação, assim como o processo de criação, requisitos, entre outras. A ISO 27002 complementa esta norma ao detalhar controlos já listados na norma 27001, de modo a facilitar a implementação de um destes sistemas.

A ISO 27005 trata a gestão de risco na segurança da informação, estabelecendo um procedimento de forma a generalizar o tratamento destes riscos. Este tratamento passa pela identificação, estimativa, avaliação, tratamento e aceitação dos riscos.

Após a definição do contexto da organização, implementação de um sistema de gestão de riscos, aplicação dos determinados controlos, e feita uma análise de risco, a organização deverá de estar muito mais próxima da conformidade com o RGPD.

This page was intetionally left blank

Lista de acrónimos

AC – *Autoridade de Controlo*

CNPD – *Comissão Nacional de Proteção de Dados*

ISO/IEC – *Organization for Standardization and the International Electrotechnical Commission*

PDCA – *Plan, Do, Check, Act*

RGPD – *Regulamento Geral de Proteção de Dados*

SGSI – *Sistema de gestão da segurança da informação*

UE – *União Europeia*

This page was intetionally left blank

Tabela de conteúdos

INTRODUÇÃO 1

1. CONTEXTUALIZAÇÃO 2

2. REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD) 1

2.1. Princípios da Integridade, da Confidencialidade e da Responsabilidade 3

3. NORMAS ISO 27000 1

3.1. ISO 27001 e 27002 - Sistemas de gestão de segurança da informação e controlos 1

3.2. ISO 27005 – Gestão de risco na segurança de informação 3

4. CONFORMIDADE COM O RGPD E NORMAS ISO 27000 1

CONCLUSÕES 1

REFERENCIAS 2

Introdução

No âmbito da unidade curricular de Políticas e Análise de Risco na Segurança de Informação, do curso de Mestrado Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, foi elaborado o presente relatório sobre o Regulamento Geral de Proteção de Dados (RGPD) e a sua implementação através da utilização da família de normas ISO 27000.

No capítulo 1 é feita uma breve contextualização acerca do RGPD e da família de normas, assim como o seu relacionamento.

No capítulo 2 é tratado o tema do RGPD de uma forma geral, dando depois enfase a alguns dos seus princípios, o da integridade, da confidencialidade e da responsabilidade.

No Capítulo 3 são abordadas as normas mais relevantes da família de normas ISO 27000, como o caso da ISO 27001, ISO 27002 e ISO 27005.

Por fim no capítulo 4 é explorada em detalhe a empregabilidade das normas desta família de modo a ajudar uma organização a entrar em conformidade com o RGPD.

1. Contextualização

Cada vez somos mais dependentes da internet, comparado há 15 anos atrás, mais de 50% da população mundial utiliza internet. [1]

Mas não foi só o número de utilizadores que aumentou, a maneira de como utilizamos a internet também mudou. Com o aparecimento das redes sociais, a quantidade de dados que enviamos aumentou drasticamente. Estes dados são na maior parte das vezes, dados pessoais, e passam por fotografias, vídeos, gostos pessoais, entre outros. Muitas das empresas por destas redes sociais, antes da regulamentação ser imposta, vendiam e ou utilizavam estes dados para publicidade personalizada. Outros sites podem ainda ter acesso a dados ainda mais confidenciais tais como cartões de crédito ou contas bancárias, sendo este o caso das lojas online.

O RGPD surgiu da necessidade de proteger as pessoas, dando poder sobre os dados aos seus titulares. Entende-se como dados pessoais qualquer dado que permita identificar direta ou indiretamente uma pessoa, como o caso do nome, morada, endereço IP, dados de localização, cartão de cidadão, passaporte, cartões de crédito, entre outros.

Muitas das empresas que se aproveitavam dos dados dos seus utilizadores tiveram agora que ser mais transparentes na forma que estas tratam os dados.

No caso de não estarem em conformidade com o regulamento, estas empresas ou organizações estarão sujeitas a coimas que podem ir até aos 20 milhões de euros. [2]

Um dos requisitos é garantir a segurança dos dados guardados, no entanto isto nem sempre é fácil de o fazer sendo que o mesmo não explica como os proteger.

As normas da família ISO 27000 são um bom ponto de partida de forma a assegurar a proteção dos dados de utilizadores. Esta família de normas revolve no tópico de segurança de informação, um aspeto que tem que ser garantido para estar em conformidade com o RGPD. Existem muitas normas pertencentes a esta família, no entanto as que se destacam são a 27000, 27001, 27002 e a 27005.

A ISO 27000 faz uma visão geral sobre o tema de segurança de informação e detalha algum do vocabulário mais técnico. [3]

Na ISO 27001 são apresentados requisitos e recomendações de uma forma geral, caso estes sejam seguidos, é possível certificar a empresa ou organização no sentido de esta estar em conformidade com a norma. [4]

A ISO 27002 contem controlos de segurança referentes às recomendações expostas na ISO 27001. [5]

Através da ISO 27005 é possível conduzir uma análise de risco, explorando assim as vulnerabilidades e potenciais ameaças existentes no sistema de gestão de informação. [6]

2. Regulamento Geral de Proteção de Dados (RGPD)

Este capítulo aborda o RGPD de uma forma geral, sendo que também é abordado mais detalhadamente os princípios da integridade, da confidencialidade e da responsabilidade.

O RGPD entrou em vigor a 25 de maio de 2018 em todos os estados-membros da União Europeia, substituindo a diretiva europeia 95/46 / CE, que tinha sido estabelecida em 1995 revogar o decreto legislativo nº196/2003.

Este regulamento aplica-se a todas as empresas da UE, a empresas que não estando na UE tratem de dados de residentes da UE ou pessoas que esteja de viagem na EU e utilizem esses dados com a finalidade de oferecer serviços ou monitorizar o comportamento destas pessoas. Na Figura 1 encontra-se uma de forma mais explícita este último segmento.

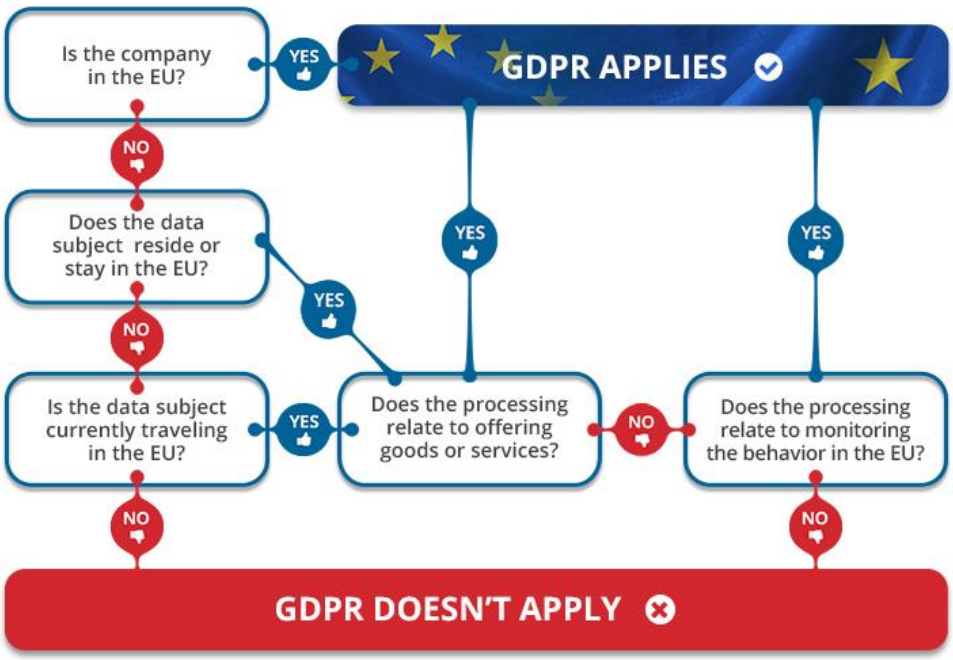

Figura 1- Aplicabilidade do RGPD a uma organização.

Os dados devem ser tratados de acordo com o consentimento dado pelo titular dos mesmos, devem estar sempre atualizados, e a organização apenas os deve de manter durante o tempo estritamente necessário.

Com o novo RGPD houve uma implementação e reforço de vários princípios como o da lealdade, o da transparência, o do consentimento e o da responsabilidade. São 11 princípios e todos eles devem estar implementados no mundo dos negócios e, consequentemente, nas empresas/organizações. Para além dos princípios, o RGPD também apresentou, de forma geral, 7 direitos aos titulares dos dados, como o direito ao acesso, à retificação, à limitação de tratamento e à oposição. Os titulares têm agora mais direitos, estando esses regulamentados e os titulares devem e têm de os conhecer, podendo usufruir deles em qualquer altura. Também possuem sempre o direito a que os seus dados pessoais se encontrem em segurança e devidamente protegidos, podendo prestar queixa a uma autoridade de controlo (AC) caso vejam os seus direitos a serem violados. A autoridade de controlo em Portugal é a Comissão Nacional de Proteção de Dados (CNPD).

Os 7 direitos a serem garantidos são: o **direito de acesso**, onde o titular dos dados tem o direito de aceder aos dados que uma organização tem sobre ele; **o direito de retificação**, em que o titular pode alterar os seus dados no caso destes se encontrarem incorretos sem necessidade de apresentar justificação; **direito a ser esquecido** que passa pela remoção dos dados do titular sem demora ou justificação no caso deste assim entender; **direito à limitação** do tratamento onde o titular dos dados pode pedir que o tratamento dos dados seja limitado; **direito à portabilidade dos dados**, em que o titular dos dados tem o direito de receber os seus dados num formato estruturado e de fácil leitura e pode ainda transmiti-los a um outro responsável de tratamento sem o impedimento do primeiro responsável; **direito à oposição**, em que o titular se pode opor em qualquer altura, a que os seus dados sejam tratados para um determinado fim; **direito à não subjeção a decisões automatizadas**, onde o titular não deverá ficar sujeito a decisão *"…tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar"*, mencionado no artigo 22, ponto 1 do RGPD.

Os 11 princípios a serem respeitados passam por: **Princípio da licitude**, onde o tratamento dos dados tem que ser sempre lícito, isto é, legal; **Princípio do consentimento**, em que os titulares dos dados podem dar ou retirar o seu consentimento no que toca a recolha de informação e/ou tratamento dos seus dados sempre que quiserem, assim como a finalidade da recolha e/ou tratamento dos dados tem que estar explícita; **Princípio da transparência**, onde a finalidade da recolha dos dados deve ser legítima, não havendo assim outras finalidades não explícitas; **Princípio da lealdade**, em que após passar uma determinada ideia

ao titular dos dados, essa ideia tem que ser mantida; **Princípio da limitação das finalidades**, onde tal como já referenciado, a finalidade dos dados recolhidos deve ser apenas a explicita inicialmente, no caso desta vir a mudar mais tarde, os titulares devem ser notificados e estes poderão optar por reverter o seu consentimento; **Princípio da minimização dos dados**, o regulamento diz especificamente que os dados recolhidos devem ser *"adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados…"* , mencionado no artigo 5, ponto 1, alínea c do RGPD; Princípio da exatidão, os dados devem ser exatos, devem de existir medidas que permitam a atualização ou remoção dos mesmos; **Princípio da limitação**, onde diz que os dados devem ser guardados de uma forma que permita a identificação do seu titular pelo período estritamente necessário de acordo com as finalidades segundo os quais foram recolhidos; **Princípio da conservação**, em que os dados podem ser guardados por um período de tempo superior se forem para fins de arquivo, interesse público, investigação científica, estatísticas, entre outros. Existem também três outros princípios, o **da integridade**, **da confidencialidade** e **da responsabilidade** que são abordados em maior detalhe no capítulo seguinte. [7]

2.1. Princípios da Integridade, da Confidencialidade e da Responsabilidade

Cabe à organização de garantir a segurança dos dados, atualizando os seus sistemas de gestão de dados sempre que haja conhecimento de uma vulnerabilidade. O responsável pelo tratamento dos dados deve de assegurar que usa as técnicas mais avançadas, dentro do que é mais adequado, de forma a *garantir "confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento"*, *"a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico"* e *"um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento"*, do artigo 32, ponto 1, alínea b, c e d do RGPD.

Relativamente aos princípios de integridade e confidencialidade, o artigo 5, ponto 1, alínea f do RGPD, refere que os dados devem ser *"tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou*

organizativas adequadas…". Desta forma as organizações têm que tomar medidas de modo a proteger os dados de serem acedidos, destruídos, danificados ou alterados de forma ilícita ou acidental.

O princípio de responsabilidade diz respeito ao responsável pelo tratamento dos dados, sendo este também responsável por respeitar o RGPD, incluindo estes princípios, assim como deve ter medidas e mecanismos que lhe permitam comprovar a conformidade com o RGPD. [7]

3. Normas ISO 27000

Para as normas da família ISO 27000, é quase sempre necessário efetuar uma contextualização da organização. Isto implica detalhar todas as informações que possam ser relevantes para através das normas ser possível encontrar os pontos críticos a serem tratados assim como os objetivos de negócio e de segurança.

Neste capítulo vão ser abordadas 3 normas pertencentes a esta família, a ISO 27001, ISO 27002 e ISO 27005.

3.1. ISO 27001 e 27002 - Sistemas de gestão de segurança da informação e controlos

A informação tem vindo a tornar-se dos ativos com maior importância para as organizações. Muitos dos negócios existentes nos dias de hoje dependem somente deste ativo, pelo que é necessário saber protegê-lo. Uma forma de assegurar isto, é utilizando um sistema de gestão de segurança de informação (SGSI).

Tendo estes sistemas sido uma mais valia para o bom funcionamento de muitos negócios, foram definidos alguns requisitos para desenvolver e operar um SGSI, de forma a possibilitar uma melhor base onde organizações poderão seguir e construir o seu sistema de gestão da segurança da informação. As normas ISO 27001 e ISO 27002 vêm ajudar no processo de criação e manutenção destes sistemas.

Para esta finalidade, a norma ISO 27001 utiliza o modelo PDCA (Plan-Do-Check-Act), que é essencialmente a base na qual os requisitos e recomendações para o desenvolvimento e operação de um SGSI assentam. Apesar de não ser referenciado na versão de 2013, o modelo PDCA é visível nas cláusulas principais. As clausulas 4 - Contexto da organização, 5 - Liderança, 6 - Planeamento, e 7 - Suporte referem ao passo *Plan*, a clausula 8 - Operação refere ao passo *Do*, a clausula 9 - Avaliação do desempenho refere ao passo *Check* e a clausula 10 - Melhoria refere ao passo *Act*.

Das clausulas pertencentes ao modelo PDCA, “Contexto da Organização”, consiste em compreender a organização e as suas finalidades e objetivos de negócio, compreender as necessidades e expetativas das partes interessadas, determinar o âmbito do sistema de gestão de segurança e a organização deverá de estabelecer, implementar, manter e melhorar de

forma contínua um sistema de segurança de informação de acordo com os requisitos desta norma. Na clausula “Liderança”, estabelece que a gestão de topo deve demonstrar liderança e comprometimento para com o SGSI, assim como devem ser estabelecidas políticas de segurança de informação apropriadas ao propósito da organização. Também são estabelecidas e atribuídas funções, responsabilidades e autoridades na organização. O “Planeamento” consiste em definir generalidades como assegurar que o SGSI possa atingir os resultados pretendidos, evitar ou reduzir os efeitos indesejáveis e atingir melhoria contínua. A organização tem que definir e aplicar um processo de avaliação do risco de segurança de informação, definir e aplicar um processo de tratamento de risco de segurança de informação e estabelecer os objetivos de segurança de informação. Na clausula “Suporte”, a organização deve determinar e proporcionar os recursos necessários para o estabelecimento, implementação, manutenção e melhoria do SGSI. A organização deverá ainda determinar as competências necessárias das pessoas que, trabalhando sobre o seu controlo, influenciam o seu desempenho de segurança de informação, assim como assegurando que estas são competentes com base numa apropriada educação. As pessoas que realizam trabalho sob o controlo da organização devem estar cientes da política de segurança de informação, da sua contribuição para a eficácia do SGSI e das implicações da não conformidade com os requisitos do SGSI. A organização deve determinar a necessidade para as comunicações internas e externas relevantes para o SGSI. A informação deve ser documentada e o seu controlo garantido. A cláusula “Operação” detalha que a organização deverá planear, implementar e controlar os processos necessários para cumprir os requisitos de segurança de informação e implementar ações definidas na cláusula 6.1. Deverão ser realizadas avaliações do risco de segurança de informação em intervalos planeados ou quando propostos. A organização deverá também implementar um plano de tratamento de risco de segurança de informação. Na cláusula “Avaliação de desempenho”, é feita uma monitorização, medição, análise e avaliação ao desempenho do sistema de segurança de informação. A organização deverá de conduzir auditorias internas em intervalos planeados para disponibilizar informação sobre se se o SGSI está conforme com requisitos da própria organização e requisitos desta norma e se está implementado e mantido com eficácia. A gestão de topo deverá rever o SGSI em intervalos planeados de modo a assegurar a sua contínua aplicabilidade, adequabilidade e eficácia. Por fim, na cláusula “Melhoria”, quando uma não conformidade ocorre, a organização deve reagir adequadamente, avaliar a necessidade de ações para eliminar causas da não conformidade de forma a eliminar repetições das mesmas, proceder a alterações no SGSI se necessário, e manter a informação

documentada como evidência. A organização deve ainda melhorar de uma forma contínua a aplicabilidade, adequabilidade e eficácia do SGSI. [4]

A norma ISO 27002, tem uma definição mais detalhada dos controlos listados no anexo a da norma ISO 27001. Estes controlos estão divididos em 13 categorias sendo estas, políticas de segurança da informação, organização de segurança da informação, segurança na gestão de recursos humanos, gestão de ativos, controlo de acesso, criptografia, segurança física e ambiental, segurança de operações, gestão de segurança de rede, aquisição, desenvolvimento e manutenção de sistemas, relações com fornecedores, gestão de incidentes de segurança da informação, aspetos de segurança da informação na gestão da continuidade do negócio, e conformidade. [5]

3.2. ISO 27005 – Gestão de risco na segurança de informação

No que toca à segurança de informação, existem três princípios fundamentais, a confidencialidade, a integridade e a disponibilidade.

A confidencialidade diz respeito ao facto de que toda a informação deve ser protegida de acordo com o seu grau de sigilo, limitando o seu acesso apenas quando necessário. A integridade passa por garantir que a informação se mantenha na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais. A disponibilidade visa que toda a informação partilhada por um indivíduo ou instituição, esteja sempre disponível aos seus utilizadores.

Uma vulnerabilidade é uma fragilidade na segurança que pode ser utilizada pelas ameaças de modo a causar danos aos ativos de uma organização. O facto de existir uma vulnerabilidade não significa que esta venha a ser explorada, no entanto devem-se tomar as devidas precauções.

Uma ameaça é composta por uma vulnerabilidade, um ator e uma motivação, podendo o ator ser um funcionário, um externo à organização ou uma organização concorrente, e a motivação ser financeira, política ou nenhuma no caso de um erro ou acidente. As ameaças podem ainda ser classificadas em 3 grupos, humanas, que estão diretamente relacionadas com as ações de indivíduos; naturais, que são decorrentes de condições da natureza tais como

terramotos, incêndios, furacões, entre outras; e ambientais, como falhas de hardware, software, dispositivos tecnológicos, bugs, entre outros. Segundo a norma ISO/IEC 27005, todas as ameaças devem ser identificadas genericamente e por tipo.

O Impacto é o resultante da ação bem-sucedida de uma ameaça, e tem uma ordem de magnitude consoante os ativos afetados. Segundo a norma ISO/IEC 27005, os impactos devem de ser especificados em torno do nível de danos ou custos causados à organização. Esta norma define que o risco é o efeito da incerteza nos objetivos e está associado ao potencial das ameaças explorarem as vulnerabilidades de um ativo ou grupo de ativos. Deve-se tratar os riscos sempre de forma preventiva, de forma a minimizar o impacto caso os mesmos se venham a concretizar.

A norma ISO/IEC 27005 estipula o processo de gestão de riscos. Este é um processo iterativo e contém várias etapas, apresentado na Figura 2. A primeira etapa é a definição do contexto, onde é estabelecida toda a informação relevante à análise e gestão de risco. Seguidamente são identificados os riscos, o que envolve a identificação de fontes, eventos causas e potenciais consequências. Depois estes são analisados, onde é compreendida a natureza dos mesmos e determinando o nível de risco. Seguidamente os riscos são avaliados, fazendo a distinção de prioridade de tratamento para cada um e são consequentemente tratados. O processo de tratamento contém 4 partes, a avaliação do tratamento já realizado, no caso de risco residual, a verificação se este é tolerável, no caso de não o ser, a definição e implementação de um novo tratamento, e a avaliação e eficácia desse tratamento. Posteriormente no caso da existência de risco residual após análise e tratamento dos mesmos, terá de existir uma aceitação do risco. [6]

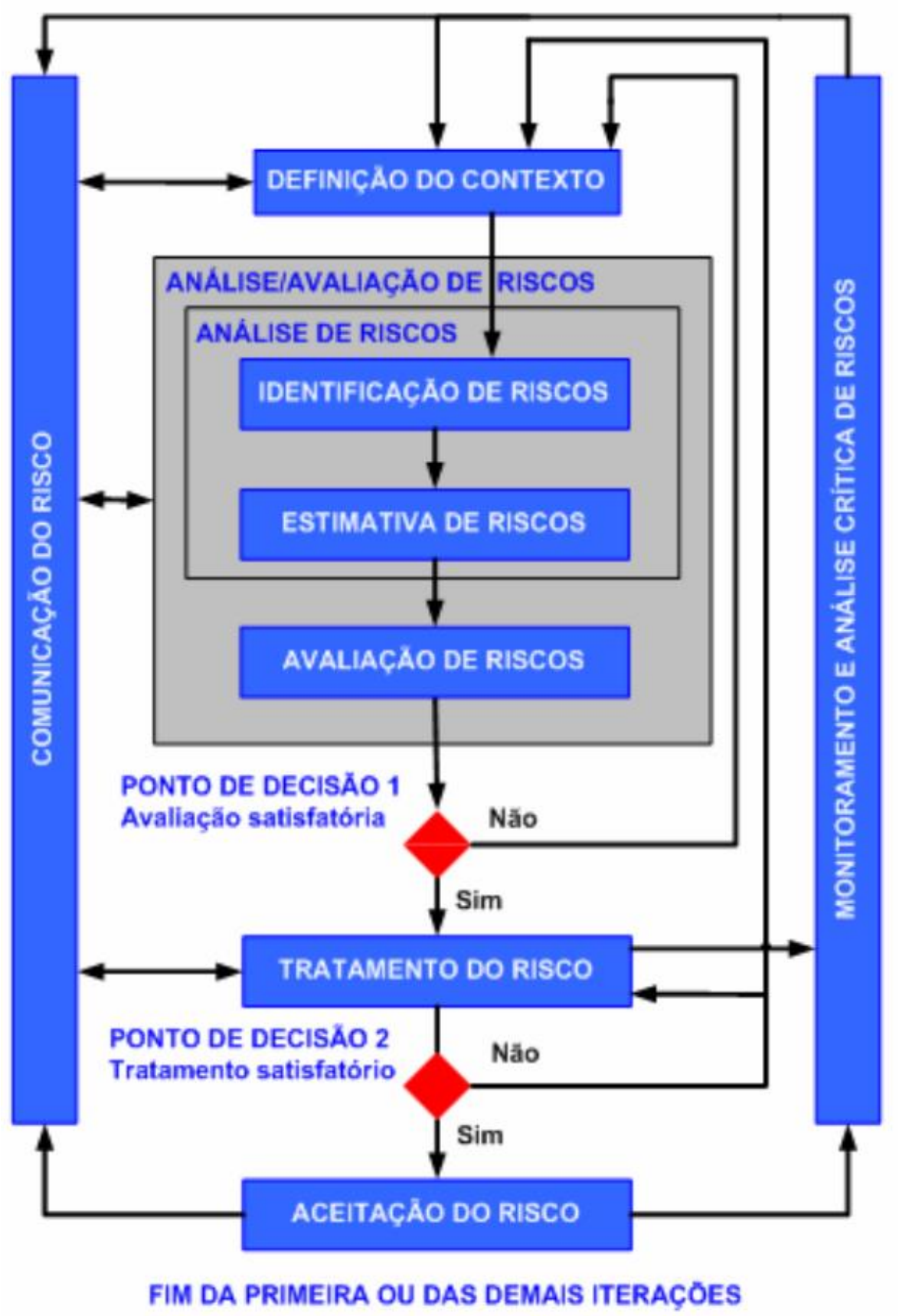

Figura 2- Processo de gestão de riscos da ISO 27005

4. Conformidade com o RGPD e normas ISO 27000

O RGPD protege um largo grupo de dados, sendo este grupo composto por vários tipos de informação pessoal, tais como nomes, IDs, números de segurança social, dados biométricos, dados médicos, opiniões políticas entre outras (Artigos 5-11). O Artigo 6 do RGPD, expressa explicitamente que as organizações necessitam de ter o consentimento dos utilizadores para poderem recolher e tratar dados sobre os mesmos, desta forma é necessário guardar um comprovativo que expresse o dito consentimento dado pelo proprietário dos dados. Segundo o artigo 33, as organizações têm também que reportar falhas de segurança durante um período de 72 horas.

Existem bastantes semelhanças no que toca a requisitos impostos pelo RGPD e recomendações especificadas pela norma ISO 27001, ISO 27002 e ISO 27005. Em termos de confidencialidade, disponibilidade e integridade dos dados, o artigo 5 do GDPR especifica os princípios generalizados para tratamento de dados tais como proteção contra acesso não autorizado ou ilícito, perda de dados acidental, destruição ou danos. O artigo 32 vem ainda especificar que as organizações têm que implementar, operar e manter medidas para garantir a segurança dos dados, tais como criptografia dos dados, resiliência de serviços de processamento e a possibilidade de restaurar os dados pessoais em tempo útil. De uma forma semelhante, a norma ISO 27001 e ISO 27002 contêm múltiplos controlos que garantem confidencialidade, disponibilidade e integridade. Na cláusula 4, "Contexto da Organização", requer que a organização identifique os problemas internos e externos que possam afetar os seus programas de segurança. A cláusula 6, Planeamento, requer que sejam determinados os objetivos de segurança e criar um programa que cumpra esses objetivos. Existem também controladores que procuram implementar medidas de segurança para garantir a confidencialidade dos dados, A.10, Criptografia.

A análise de risco a sistemas de segurança de informação é obrigatória tanto no RGPD como na ISO 27001. O artigo 35 do RGPD requer que as organizações conduzam avaliações de impacto sobre a proteção de dados e identificações de riscos a dados de indivíduos. A ISO 27001 aconselha as organizações a efetuar analises de risco detalhadas, de modo a identificar ameaças e vulnerabilidades que possam afetar os seus ativos (Cláusula 6.1.2), e selecionar medidas de segurança apropriadas de acordo com os resultados de dita análise

(Cláusula 6.1.3). De modo a efetuar uma análise de risco detalhada e correta, deve-se seguir a norma ISO 27005, pois esta detalha um processo de análise de risco definido assim como várias recomendações de como proceder a uma análise de risco.

A gestão de parceiros de negócio é um requerimento da cláusula 8 da ISO 27001, Operação, onde é necessário identificar todas as ações efetuadas por *outsourcing* e garantir que estas são controladas. A cláusula A.15, "Segurança da informação nas relações com os fornecedores", providencia orientação para as relações com fornecedores e requer que as organizações monitorizem e analisem o serviço de entrega. O artigo 28 do RGPD também requer controladores para garantir os termos contratuais e garantias com os processadores de informação, criando assim um acordo de processamento de informação.

De acordo com os artigos 33 e 34 do RGPD, as organizações têm que notificar as autoridades num período de 72 horas após a descoberta de uma violação de dados pessoais. Os proprietários dos dados também têm que ser notificados, mas só no caso de a informação comprometida compor um alto risco para os direitos e liberdade dos proprietários. A cláusula A.16 da ISO 27001, "Gestão de incidentes de segurança da informação", não especifica a janela de tempo para notificação de violação de dados, mas aconselha a que as organizações reportem estes incidentes o mais cedo possível.

O artigo 25 do RGPD requer que as organizações implementem medidas técnicas e organizacionais durante o processo de design de todos os projetos de modo a garantir a privacidade dos dados desde o início. Na ISO 27001 também existem recomendações semelhantes. Na cláusula 4, Contexto da organização, é recomendado que as organizações entendam o escopo e contexto da informação que recolhem e tratam, enquanto que a cláusula 6, Planeamento, recomenda que sejam efetuadas análises de risco regulares de modo a garantir a eficácia do seu sistema de gestão de segurança de informação.

O artigo 30 do RGPD requer que as organizações mantenham registos das suas atividades de processamento incluindo categorias de informação, finalidade de recolha e descrição geral de dados técnicos e medidas de segurança organizacionais. De forma semelhante, a ISO 27001 dita que as organizações devem documentar os seus processos de segurança assim como os resultados das análises de risco e tratamento de risco (Cláusula 8, Operação). De acordo com o controlo A.8, responsabilidade pelos ativos, os ativos devem ser listados e classificado, e os gestores dos ativos devem ser atribuídos.

No entanto apesar destas normas cobrirem bastantes requisitos para obter conformidade com o RGPD, existem muitos outros que não são abordados, como o caso de requisitos relacionados com a privacidade dos dados, detalhados no artigo 3 do RGPD (Diretos dos titulares dos dados). [8]

Conclusões

Com a introdução do regulamento geral de proteção de dados e as suas exigências, muitas organizações têm ainda muitas dificuldades em manter conformidade com o mesmo. Existem muitos direitos a conceder aos utilizadores e muitos princípios a serem implementados, pelo que se torna um processo difícil de assegurar conformidade com todos os requisitos do regulamento. Um dos requisitos mais importantes é a garantia da proteção dos dados dos utilizadores, proteção essa que assenta nos pilares da segurança da informação, a confidencialidade, disponibilidade e integridade.

A família de normas ISO 27000 foca-se no tema da segurança da informação e contem algumas normas que podem facilitar bastante em alcançar a conformidade com o RGPD, como é o caso da ISO 27001, que explica de um modo geral o funcionamento de sistema de gestão de segurança de informação, sistema este que detalha políticas de segurança de forma a minimizar riscos, a ISO 27002 que aborda o tema da norma anterior em maior detalhe e a ISO 27005 que detalha o processo de uma análise de risco onde se procura minimizar o risco da segurança da informação, análise esta que é uma das recomendações da ISO 27001. Para além da ISO 27001 ser uma norma com recomendações a seguir, esta também pode ser utilizada para se obter uma certificação de conformidade com a própria norma. Não sendo um requerimento para estar em conformidade com o RGPD, obter uma certificação ISO 27001 é meio caminho andado.

Referencias

[1] "Internet World Stats," [Online]. Available: https://www.internetworldstats.com/emarketing.htm. [Acedido em 15 1 2019].

[2] "GDPR EU," [Online]. Available: https://www.gdpreu.org/compliance/fines-and-penalties/. [Acedido em 16 1 2019].

[3] ISO/IEC 27000:2014, Information technology - Security techniques - Information security management systems - Overview and vocabulary.

[4] NP ISO/IEC 27001:2013, Tecnologia de informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos.

[5] ISO/IEC 27002:2013, Information technology - Security tecniques - Code of practice for information security management.

[6] NP ISO/IEC 27005:2011, Tecnologia de informação - Técnicas de segurança - Gestão de Riscos de Segurança da Informação.

[7] "REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO," *Jornal Oficial da União Europeia,* 2016.

[8] M. Middleton-Leal, "GDPR and ISO 27001," Netwrix Blog, [Online]. Available: https://blog.netwrix.com/2018/04/26/gdpr-and-iso-27001-mapping-is-iso-27001-enough-for-gdpr-compliance/. [Acedido em 17 1 2019].