CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Guia para
Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança

v1.1 dezembro 2022
Centro Nacional de
Cibersegurança

GOVEIN 19
Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia

ÍNDICE

I. SUMÁRIO EXECUTIVO

A consciencialização e a implementação de medidas de segurança da informação e cibersegurança nas organizações, bem como o compromisso da gestão de topo neste âmbito, são cada vez mais fundamentais nos dias que correm.

A utilização de meios tecnológicos pelas organizações para suportar os seus processos de negócio, a disponibilização de informação aos clientes, profissionais e cidadãos através do digital e a existência de um maior número de dispositivos conectados entre si através da internet, aumentam a exposição ao risco e a ameaças no ciberespaço, que devem ser endereçadas de forma preventiva, através de uma abordagem de gestão dos riscos.

Um ambiente seguro é fundamental para estabelecer e desenvolver qualquer atividade económica ou social, devendo a cibersegurança, em todas as suas vertentes, ser um fator a considerar nas sociedades atuais.

Em alinhamento com o disposto no Regime Jurídico da Segurança do Ciberespaço e com o Decreto-Lei n.º 65/2021, de 30 de julho, este documento tem como objetivo ser um instrumento que auxilia as organizações na realização de um processo de gestão dos riscos em matérias de segurança da informação e cibersegurança, tendo sido baseado em referenciais e boas práticas de referência. No entanto, este Guia não impede que as organizações adotem outros referenciais e metodologias para realizar uma análise dos riscos nos termos dos artigos 9.º e 10.º do Decreto-Lei nº65/2021, de 30 de julho, que possam estar mais alinhadas com os seus objetivos e contexto organizacional.

Através deste referencial, pretende-se que as organizações caracterizem a sua situação atual, definam objetivos e elenquem um conjunto de ações e medidas que fomentem uma evolução positiva dos riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam. A quem o aplica, será possível a definição e implementação de medidas e controlos de segurança ao nível técnico e organizativo para garantir um nível de segurança adequado ao risco em causa, promovendo, ao longo do tempo, melhorias na gestão dos riscos.

II. INTRODUÇÃO

A. ENQUADRAMENTO

O Guia para Gestão dos Riscos em matérias de segurança da informação e cibersegurança tem como objetivo definir uma abordagem de referência sistematizada e coerente ao processo de identificação, análise, avaliação e tratamento periódico dos riscos e de aferição da forma como estes se relacionam no âmbito do fornecimento de bens e/ou prestação de serviços.

Este Guia pretende, assim, constituir-se um **referencial** e orientar as diversas entidades nacionais para a realização de um processo de gestão dos riscos ao nível organizacional, tendo em conta os objetivos específicos que permitam garantir a manutenção da confidencialidade, integridade e disponibilidade da informação. Esta metodologia de gestão dos riscos pretende igualmente servir de base orientadora aos requisitos expressos no âmbito da aplicação da Lei n.º 46/2018 de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC) transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, e respetivo Decreto-Lei n.º 65/2021, de 30 de julho que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019.

Todas as entidades abrangidas por este último diploma devem, de acordo com o artigo 10.º realizar uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam e, no caso dos operadores de serviços essenciais, também em relação aos ativos que garantam a prestação dos serviços essenciais. Na sequência de cada análise dos riscos, as entidades devem adotar as medidas técnicas e organizativas adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.

Neste contexto, entenda-se "risco" como "*uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação*". Sendo uma característica intrínseca do risco o facto de este não poder ser totalmente eliminado, é fundamental a definição e operacionalização de uma estratégia organizacional transversal para garantir a implementação de um processo eficaz e sistematizado de gestão dos riscos, numa lógica de melhoria contínua.

Através de um processo permanente e contínuo de identificação, quantificação, diagnóstico e resposta aos riscos, é possível, as organizações identificarem possíveis ameaças que possam explorar as vulnerabilidades dos ativos, bem como quais os níveis do risco associados, avaliando-se, assim, a probabilidade de ocorrência e possíveis impactos.

Através das diretrizes já estabelecidas no Quadro Nacional de Referência para a Cibersegurança e do RJSC, este Guia vem constituir um aspeto determinante para auxiliar as organizações na escolha das **medidas e controlos de segurança a definir e implementar ao nível técnico e organizativo para garantir um nível de segurança adequado ao risco em causa.**

B. CONTEXTO LEGISLATIVO E REFERENCIAL

a) Contexto Legislativo

A **Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho,** aprovada em 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União - e mais conhecida por Diretiva SRI – Diretiva relativa à segurança das redes e da informação - é o primeiro instrumento do mercado interno que tem por objetivo melhorar a resiliência da União Europeia (UE) contra os riscos de cibersegurança. Introduzindo medidas concretas destinadas a reforçar as capacidades em matéria de cibersegurança em toda a UE e a atenuar as ameaças crescentes às redes e aos sistemas de informação utilizados para a prestação de serviços essenciais em setores-chave, tem como objetivo promover uma cultura de gestão dos riscos entre todo o tipo de entidades, incluindo empresas.

A **Lei n.º 46/2018 de 13 de agosto,** que estabelece o Regime Jurídico da Segurança do Ciberespaço, transpõe a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016 para o âmbito nacional. Esta Lei aplica-se a entidades da Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais dos setores da energia, transportes, bancário, infraestruturas do mercado financeiro, saúde, fornecimento e distribuição de água potável e infraestruturas digitais, aos prestadores de serviços digitais, bem como a quaisquer outras entidades que utilizem redes e sistemas de informação, nomeadamente no que concerne à notificação voluntária de incidentes.

Com a publicação do **Decreto-Lei n.º 65/2021 de 30 de julho,** procedeu-se à regulamentação dos aspetos remetidos para legislação complementar na Lei n.º 46/2018, de 13 de agosto, sido estabelecidos os requisitos de segurança das redes e sistemas de informação e de notificação de incidentes que devem ser cumpridos pelas entidades identificadas no RJSC. Além disso, o Decreto-Lei em causa determina ainda que o Centro Nacional de Cibersegurança é a Autoridade Nacional de Certificação da Cibersegurança, o que permite a nível nacional a implementação do Regulamento (UE) 2019/881 do Parlamento e do Conselho, de 17 de abril de 2019, referente à certificação de cibersegurança de produtos, serviços e processos de tecnologias de informação.

No âmbito deste Guia, é de particular interesse o **Artigo 10.º** do Decreto-Lei n.º 65/2021 de 30 de julho, que estabelece que as entidades da Administração Pública, os operadores de infraestruturas críticos e operadores de serviços essenciais devem realizar uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam e, no caso de operadores de serviços essenciais, também em relação aos ativos que garantam a prestação dos serviços essenciais.

A Análise dos riscos de **âmbito global** deve ser realizada, pelo menos, uma vez por ano. Em relação ao **âmbito parcial**, esta deve ser realizada durante o planeamento e preparação da introdução de uma alteração ao ativo ou ativos, em relação ao ativo ou ativos envolvidos; ou após a ocorrência de um incidente com impacto relevante; ou outra situação extraordinária, em relação aos ativos afetados.

Deve ser sempre realizada uma análise dos riscos de âmbito global ou parcial após a notificação, por parte do CNCS, de um risco, de uma ameaça ou de uma vulnerabilidade emergentes que impliquem uma elevada probabilidade de ocorrência de um incidente com impacto relevante, dentro do prazo fixado pelo CNCS.

Na sequência de cada análise dos riscos, as entidades devem adotar as medidas técnicas e organizativas adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.

b) Contexto Referencial

Também relevante para o contexto referencial e desenvolvimento do presente Guia, foram consultados os pressupostos e boas práticas descritos no QNRCS, e os principais referenciais em matérias de gestão dos riscos como ISO/IEC 27005[1] e NP ISO/IEC 31000[2].

O **QNRCS**, desenvolvido e disponibilizado pelo Centro Nacional de Cibersegurança, reúne um conjunto das melhores práticas que permitem às organizações reduzir o risco associado às ciberameaças, disponibilizando as bases para que qualquer entidade possa, de uma forma voluntária, cumprir os requisitos mínimos de segurança das redes e sistemas de informação... Este documento apresenta um conjunto de recomendações com vista à implementação de medidas de Identificação, Proteção, Deteção, Resposta e Recuperação contra ameaças que colocam em causa a cibersegurança da organização, envolvendo toda a sua estrutura e tendo em consideração os aspetos humanos, tecnológicos e processuais.

A **ISO/IEC 31000** disponibiliza um conjunto de princípios e de orientações genéricas sobre gestão dos riscos para as organizações. Por outro lado, a **ISO/IEC 27005** especifica orientações e processos para gestão dos riscos de segurança dos sistemas de informação de uma organização, suportando-se, em particular, nos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI), implementado de acordo com a norma ISO/IEC 27001[3]. A ISO/IEC 27005 não fornece uma metodologia específica para a gestão dos riscos de segurança da informação, cabendo às organizações definirem qual a sua abordagem para a gestão dos riscos.

1 ISO/IEC 27005 – Information Technology – Security techniques – Information security risk management
2 NP ISO/IEC 31000 – Gestão do Risco – Linhas de orientação
3 NP ISO/IEC 27001 – Tenologia de Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos

É, assim neste contexto que é disponibilizado o Guia para Gestão dos Riscos que aqui se apresenta, representando o mesmo uma metodologia que, de entre outras, segue as melhores práticas de mercado. Este, porém, **não impede que as organizações adotem outras referências que possam estar mais alinhadas com os seus objetivos e contexto organizacional**.

C. PÚBLICO-ALVO

Este Guia para Gestão dos Riscos pretende ser um referencial cujo público-alvo são as entidades abrangidas pelo RJSC e Decreto-Lei n.º 65/2021, de 30 de julho, no qual se inserem as entidades da Administração Pública, Operadores de Infraestruturas Críticas, Operadores de Serviços Essenciais e Prestadores de Serviços Digitais. No entanto, sendo um documento público, não exclui a sua utilização por toda a sociedade e todo o tipo de organizações que pretendam tirar benefício deste documento.

D. DEFINIÇÕES E ABREVIATURAS

a) Definições

Na tabela seguinte identificam-se os termos utilizados ao longo do documento, cuja definição importa apresentar.

Sempre que aplicável, são usados termos definidos em normas ou legislação nacional em vigor. Na coluna "Origem" é indicada a norma, referencial ou legislação onde o termo se encontra definido.

Tabela 1 - Definições

TERMO	DEFINIÇÃO	ORIGEM
Ameaça	Potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização	ISO/IEC 27032
Ativo	Todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços.	Instrução Técnica – Regulamento nº183/2022
Confidencialidade	Propriedade de que as informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados	ISO/IEC 27000
Consequência	Resultado de um evento que afeta os objetivos	ISO 73:2009
Controlos	Conjunto de medidas que permite modificar o risco	ISO/IEC 27000
Disponibilidade	Propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada	ISO/IEC 27000
Evento	Ocorrência ou alteração de um conjunto particular de circunstâncias	ISO 73:2009
Impacto	Resultado decorrente da verificação de um determinado evento de segurança sobre um ou mais recursos, evento este que se traduz normalmente em consequências diretas ou indiretas, para os recursos mencionados	
Incidente	Um evento com um efeito adverso real na segurança das redes e dos sistemas de informação	Lei n.º 46/2018, 13 de julho

TERMO	DEFINIÇÃO	ORIGEM
Integridade	Propriedade de precisão e completude	ISO/IEC 27000
Probabilidade	Frequência expectável de acontecer o evento de risco num determinado período	
Risco	Uma circunstância ou um evento razoavelmente identificável, com um efeito adverso potencial na segurança das redes e dos sistemas de informação.	Lei n.º 46/2018, 13 de julho
Risco atual	Representado pela quantidade de risco que existe com os controlos existentes no momento da identificação dos riscos.	
Risco inerente	Representado pela quantidade de risco existente sem qualquer tipo de controlos existentes associados	
Risco residual	Representado pela quantidade de risco que permanece ou que aparece após a inclusão dos controlos adicionais e/ou ajustes dos controlos já existentes	
Vulnerabilidade	Fraqueza de um ativo ou controlo que pode ser explorada por uma ou mais ameaças.	ISO/IEC 27000
Parte interessada	Pessoa ou organização que pode afetar, ser afetada por, ou considerar-se como sendo afetada por uma decisão ou atividade. Pode ser um indivíduo ou um grupo que tem um interesse em qualquer decisão ou atividade de uma organização.	NP EN ISO 22301
Pentesting	Teste de intrusão para verificar o nível de segurança das redes e sistemas, utilizando diferentes tipos de ataques realizados por analistas de segurança, devidamente autorizados.	ENISA[4]
Sistema de Gestãode Segurança da Informação (SGSI)	Inclui estratégias, planos, políticas, medidas, controlos, e diversos instrumentos usados para estabelecer, implementar, operar, monitorizar, analisar criticamente, manter e melhorar a segurança da informação	ISO/IEC 27000

b) Abreviaturas

Tabela 2 - Abreviaturas

ABREVIATURA	DEFINIÇÃO
CISO	*Chief Information Security Officer* – Responsável de Segurança de Informação.
COO	*Chief Operations Officer* – Responsável das Operações
ISO	*International Organization for Standardization* - Organização internacional de normalização
ISO/IEC	*International Organization for Standardization/International Electrotechnical Commission* – Organização internacional de normalização/Comissão eletrotécnica internacional.
QNRCS	Quadro Nacional de Referência para a Cibersegurança
OES	Operadores de Serviços Essenciais
RJSC	Regime Jurídico da Segurança do Ciberespaço, estabelecido pela Lei nº46/2018, de 13 de agosto.
SGSI	Sistema de Gestão de Segurança da Informação.
TIC	Tecnologias de Informação e Comunicação

4 Consultar em https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits

E. ESTRUTURA DO DOCUMENTO

O documento encontra-se estruturado através de sete macro secções.

Na sua parte inicial efetua-se uma **INTRODUÇÃO** ao Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança, identificando-se o seu enquadramento, o seu contexto legislativo e referencial, o seu público-alvo, e as definições e abreviaturas das terminologias utilizadas ao longo do documento.

No capítulo "**GESTÃO DOS RISCOS**" apresenta-se a primeira fase do processo de gestão dos riscos com o estabelecimento do contexto. Neste define-se o âmbito e critérios básicos a considerar para a gestão do risco de segurança da informação e da cibersegurança e a implementação processual orientada à gestão dos riscos, que permite às organizações a tomada de decisões de forma priorizada e informada.

De seguida é apresentado o capítulo "**PROCESSO DE LEVANTAMENTO DOS RISCOS**" que identifica, reconhece, quantifica e descreve os riscos e pretende capacitar as organizações a avaliá-los e priorizá-los de acordo com a sua gravidade percebida e com outros critérios estabelecidos. O processo de levantamento dos riscos decompõe-se nas seguintes atividades:

- identificação do risco (etapa 1);
- análise do risco (etapa 2);
- avaliação do risco (etapa 3).

No capítulo "**TRATAMENTO DO RISCO**" envolve a identificação, formalização e implementação de um ou mais planos de ação, os quais têm como objetivo controlar e/ou mitigar as causas dos riscos identificadas na fase de anterior.

No capítulo "**COMUNICAÇÃO E CONSULTA DO RISCO**" são apresentadas atividades que têm como objetivo alcançar o consenso sobre como gerir os riscos de segurança da informação e cibersegurança, através da troca e/ou partilha das informações entre os responsáveis e as outras partes interessadas.

No capítulo "**MONITORIZAÇÃO E REVISÃO DOS RISCOS**" indica que o departamento responsável pela gestão dos riscos da organização tem a responsabilidade de monitorizar, com regularidade, o ambiente da organização, de forma que se identifique atempadamente qualquer alteração que possa ter existido no contexto e que se possa traduzir numa alteração à perceção do risco.

No capítulo **"DOCUMENTAÇÃO E REGISTO DOS PROCESSOS E RESULTADOS"** é relevada a importância do registo e documentação de todos os processos levados a cabo e respetivos resultados obtidos ao logo do processo de gestão dos riscos, não só para fins de evidência em processos de certificação e de supervisão como para garantir um processo de melhoria contínua interno.

No final do documento, é apresentado um **Exemplo** através da aplicação da metodologia descrita neste Guia, assim como os respetivos **Anexos** relevantes ao documento.

III. GESTÃO DOS RISCOS

A. CONSIDERAÇÕES INICIAIS

A implementação processual orientada à gestão dos riscos permite às organizações a tomada de decisões de forma priorizada e informada. Estas decisões devem estar sempre igualmente orientadas à garantia da confidencialidade, disponibilidade e integridade no fornecimento de bens e/ou prestação de serviços.

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

A gestão dos riscos de uma organização pode ser entendida como a gestão do efeito da incerteza nos objetivos organizacionais e determinação das ações necessárias, para que esses efeitos (verosimilhança e consequência) possam ser minimizados para níveis considerados aceitáveis por parte da organização.

Neste sentido, importa introduzir e/ou reforçar alguns conceitos importantes relacionados com a gestão dos riscos:

- Ameaça: Potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização.
- Vulnerabilidade: Fraqueza de um ativo ou controlo que pode ser explorada por uma ou mais ameaças.
- Impacto: Prende-se com o resultado decorrente da verificação de um determinado evento de segurança sobre um ou mais recursos, evento este que se traduz normalmente em consequências diretas ou indiretas, para os recursos mencionados.
- Risco: Uma circunstância ou um evento razoavelmente identificável, com um efeito potencial adverso na segurança das redes e dos sistemas de informação.

O processo de gestão dos riscos é um exercício estruturado, no qual a organização identifica possíveis ameaças que se possam explorar as vulnerabilidades dos ativos, bem como quais os níveis do risco associado, avaliando-se a probabilidade de ocorrência e possíveis impactos.

A **Figura 1** ilustra estes conceitos e relações de alto nível.

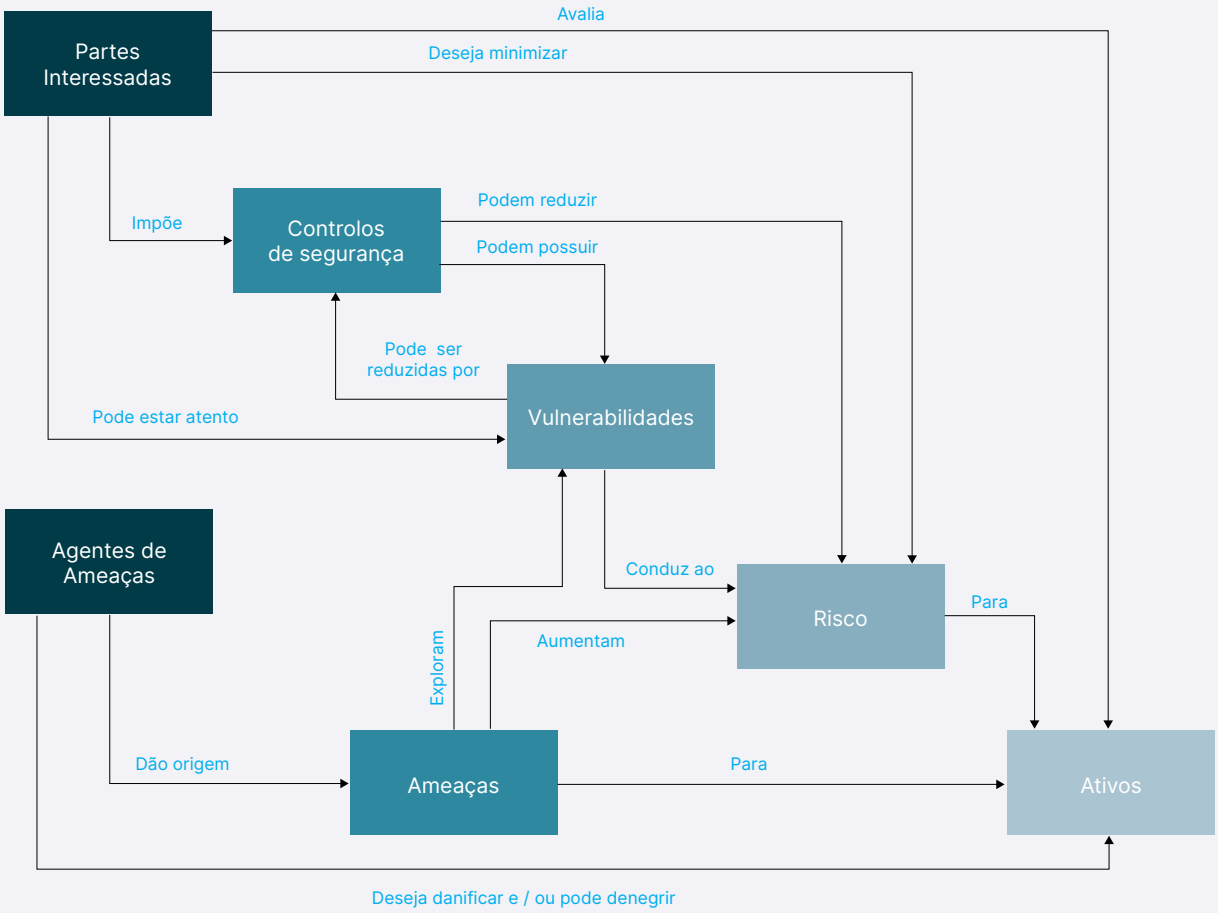

Figura 1 – Conceitos de segurança e as suas relações - adaptação da Norma ISO/ IEC 15408-1

A **Figura 2** apresenta o processo de gestão dos riscos que será utilizado neste Guia, sendo composta pelas seguintes fases:

- Estabelecer Contexto;
- Levantamento dos Riscos (que inclui a identificação, análise e avaliação do risco);
- Tratamento do risco;
- Aceitação do Risco;
- Dando-se depois, e de forma contínua, sequência às fases de Comunicação e Consulta e de Monitorização e Revisão do Risco.

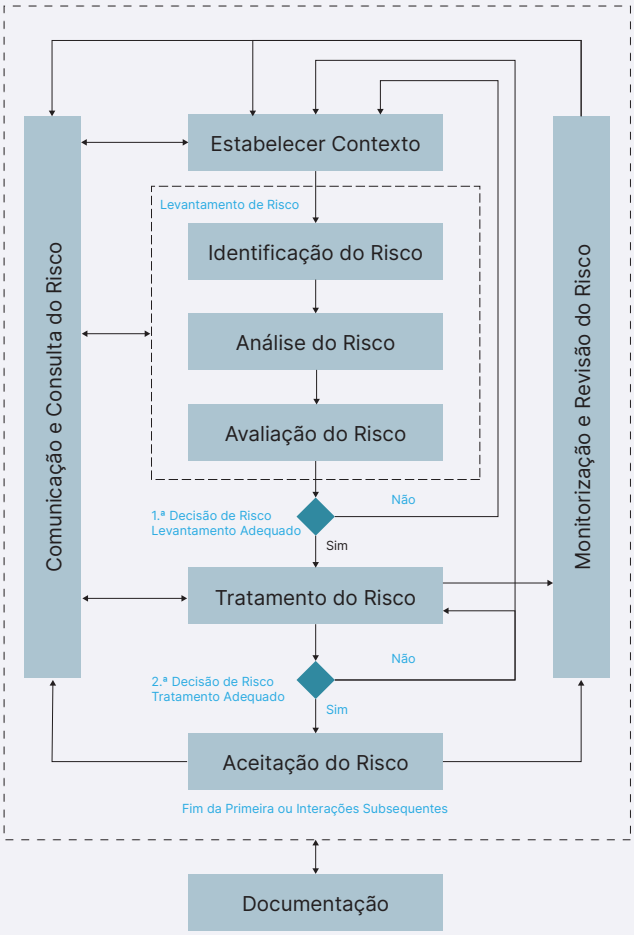

Figura 2 - Processo de Gestão dos Riscos; Fonte: ISO/IEC 27005

Em síntese, a gestão dos riscos é sistemática, estruturada e oportuna, procurando sempre a implementação de uma melhoria contínua do processo.

B. ESTABELECER O CONTEXTO

A fase de **Estabelecer o Contexto** no processo de gestão dos riscos é essencial para o planeamento e implementação do mesmo, uma vez que permite compreender os critérios, decisões e recursos internos e externos relevantes ao propósito da organização, e que possam afetar a sua capacidade de alcançar os objetivos definidos.

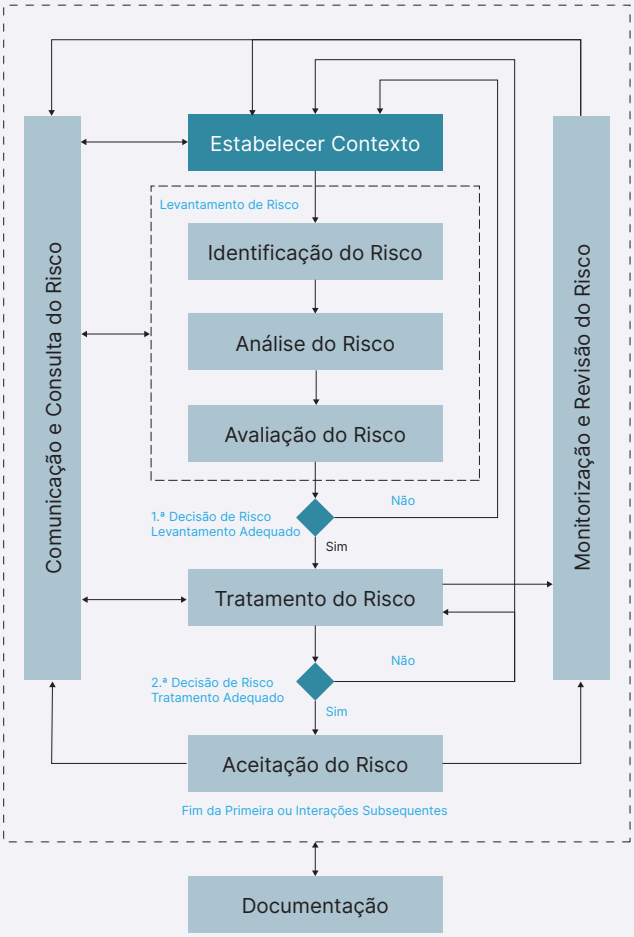

Figura 3 - "Estabelecer Contexto"- Processo de Gestão dos Riscos; Fonte: ISO/IEC 27005

De uma forma prévia, a organização deve identificar os recursos humanos como partes interessadas internas e/ou externas, assim como definir as suas funções e responsabilidades para a gestão dos riscos de segurança da informação e cibersegurança. A título exemplificativo, a **Tabela 3** distribui as funções e responsabilidades de risco num contexto organizacional.

Tabela 3 - Funções e responsabilidades

FUNÇÃO	RESPONSÁVEL	RESPONSABILIDADES
Gestão de Topo	Chefia da organização responsável pelas decisões superiores	• Analisar e aprovar todas as decisões tomadas no processo de gestão dos riscos; • Delegar funções dentro da organização no que diz respeito ao processo de gestão dos riscos.
Gestor de Risco	Responsável intermédio que gere o risco na organização, de forma transversal	• Controlar o processo de gestão dos riscos da organização; • Assegurar a recolha de toda a informação necessária para a identificação e análise do risco; • Realizar a análise dos riscos; • Assegurar que as opções escolhidas para tratar os riscos são as mais corretas e/ou oportunas; • Assegurar que o processo de gestão dos riscos se mantém compatível com a política, objetivos e com os demais requisitos legais e regulatórios aplicáveis à organização; • Assegurar que o processo interno da gestão dos riscos é comunicado a todos os colaboradores com funções relevantes para a sua aplicação.
Dono do Risco	Pessoa ou organização contratante que gere diretamente cada um dos ativos sujeitos ao processo de gestão dos riscos	• Gerir os ativos ou sistemas de informação e os seus respetivos riscos; • Participar no processo de gestão e análise dos riscos; • Assegurar que todos os riscos são reportados ao Gestor do Risco; • Assegurar que o risco é identificado, analisado, avaliado e tratado; • Assegurar que as opções e ações de tratamento são cumpridas e implementadas.

Note-se que identificando o modelo de governação mais adequado para a realidade organizacional, é necessário também definir processo de escalonamento associado, assim como os critérios de aceitação do risco, nomeadamente estabelecendo a partir de que nível será necessária a aprovação da gestão de todo para que o mesmo possa ser aceite.

Além dos recursos humanos, é também nesta fase que devem ser identificados os recursos materiais que garantirão a correta execução de todo o restante processo, como ferramentas de suporte e procedimentos para a gestão, análise e tratamento dos riscos.

Outra atividade de real importância nesta fase inicial é a definição do âmbito e fronteiras do processo de gestão dos riscos que irá ocorrer, definindo e delimitando todos os pontos fronteira, os quais deverão ser devidamente fundamentados. Podem ser exemplos de definição de âmbito para um processo de gestão dos riscos o edifício/localização; departamento; plataforma de infraestrutura; plataforma aplicacional ou os processos ou um conjunto de processos específico referentes à atividade da organização.

A **Tabela 4** apresenta o exemplo de um processo a ser implementado na atividade de 'Estabelecer Contexto'.

Tabela 4 - Exemplo de um processo de "Estabelecer o contexto"

ESTABELECER O CONTEXTO		
Entradas (*Inputs*)	**Atividades**	**Saídas (*Outputs*)**
• Visão e obrigações da organização • Objetivos da organização em matérias de requisitos de segurança da informação e cibersegurança • Necessidades e expectativas das partes interessadas • Visões das partes interessadas • Ferramentas e técnicas de aferição dos riscos	• Definição do âmbito e fronteiras do processo de gestão do risco • Identificação dos registos a criar e manter (ex. atas de reuniões, relatórios de progresso, etc.) • Identificar o modelo de governação a aplicar no processo de gestão dos riscos e definir um processo de escalonamento e responsabilidade apropriado • Definir os papéis e responsabilidades das partes interessadas internas e externas	• Âmbito e fronteiras documentadas • Abordagem ao risco definida. • Matriz RACI do processo de gestão do risco • Critérios de aceitação do risco

Concluindo, nesta etapa de 'Estabelecer Contexto' devem ser definidos os objetivos, estratégias, âmbito, fronteiras e os parâmetros das atividades das organizações ou das partes da organização em que o processo de gestão dos riscos será aplicado, assim como os recursos necessários para a operacionalização do mesmo. É também nesta fase que deve ser estabelecido o nível de risco aceitável pela organização, através dos critérios de aceitação do risco.

É importante que todas as decisões tomadas no decorrer desta etapa sejam devidamente aprovadas pela Gestão de Topo da organização.

a) Matriz RACI

A matriz RACI ou matriz de responsabilidades possibilita que os vários envolvidos conheçam as suas responsabilidades no ciclo de vida de um projeto ou processo.

Geralmente diversas partes interessadas são envolvidas no processo de gestão do risco, conforme apropriado e nos momentos determinados, permitindo uma partilha de conhecimento, visão e perceções abrangentes sobre o risco. Para assegurar este envolvimento, a organização deve definir um modelo de governação/organizacional de gestão do risco, no qual se detalha os diversos níveis de responsabilização e envolvimento das partes interessadas, nomeadamente através de uma matriz do tipo RACI. Esta contribui para uma melhoria da consciencialização e numa gestão do risco e tomada de decisão mais informada.

Os tipos de participação RACI usados são:

- **R**(*esponsible*) – Responsável pela execução da tarefa. Parte interessada responsável, operacionalmente, pela satisfação da atividade e pela criação do resultado pretendido.
- **A**(*ccountable*) – Responsável pelo sucesso da tarefa. Como princípio, o *Accountable* é único. O *Accountable* recebe sempre informação apropriada para supervisionar a tarefa, mas também poderá ter atividades operacionais na execução da tarefa. É geralmente quem revê e entrega a tarefa antes de ser considerada como concluída.
- **C**(*onsulted*) – Fornece informação para a tarefa, nomeadamente esclarecendo impactos do projeto no seu trabalho ou domínio de atividade.
- **I**(*nformed*) – Recebe informação da tarefa, nomeadamente sobre o progresso da atividade, não necessitando dos detalhes associados.

Tabela 5 - Matriz RACI: Exemplo

MATRIZ RACI - EXEMPLO			
Atividades	**Gestão de Topo**	**Gestor do Risco**	**Dono do Risco**
Atividade A	I	R, A	R, C
Atividade B	I	A	R
Atividade C	R	C	I

IV. PROCESSO DE LEVANTAMENTO DOS RISCOS

O processo de **Levantamento dos Riscos** identifica, quantifica e descreve os riscos e capacita as organizações a priorizá-los de acordo com a sua gravidade percecionada, ou com outros critérios estabelecidos.

O processo de levantamento dos riscos consiste nas seguintes atividades:

- Identificação dos riscos (etapa 1);
- Análise dos riscos (etapa 2);
- Avaliação dos riscos (etapa 3).

São objetivos desta fase determinar o valor dos ativos de informação, identificar as ameaças e vulnerabilidades existentes (ou que possam existir), identificar os controlos existentes e os seus efeitos no risco identificado, determinar as consequências ou impactos possíveis e, por último, priorizar os riscos derivados.

A etapa de avaliação dos riscos é executada frequentemente em duas (ou mais) iterações. Inicialmente, é realizada uma avaliação de alto nível para identificar os riscos potencialmente altos, os quais merecem uma segunda iteração para avaliar com maior profundidade. Existindo necessidade, poderão ser realizadas análises adicionais, de forma a complementar a avaliação do risco.

ETAPA 1 - IDENTIFICAÇÃO DOS RISCOS

A fase de 'Identificação dos Riscos' é a primeira etapa do processo de levantamento dos riscos.

O propósito da **Identificação dos Riscos** é determinar as ocorrências que poderão causar uma potencial perda à organização avaliando o como, onde e o porquê desta perda poder acontecer.

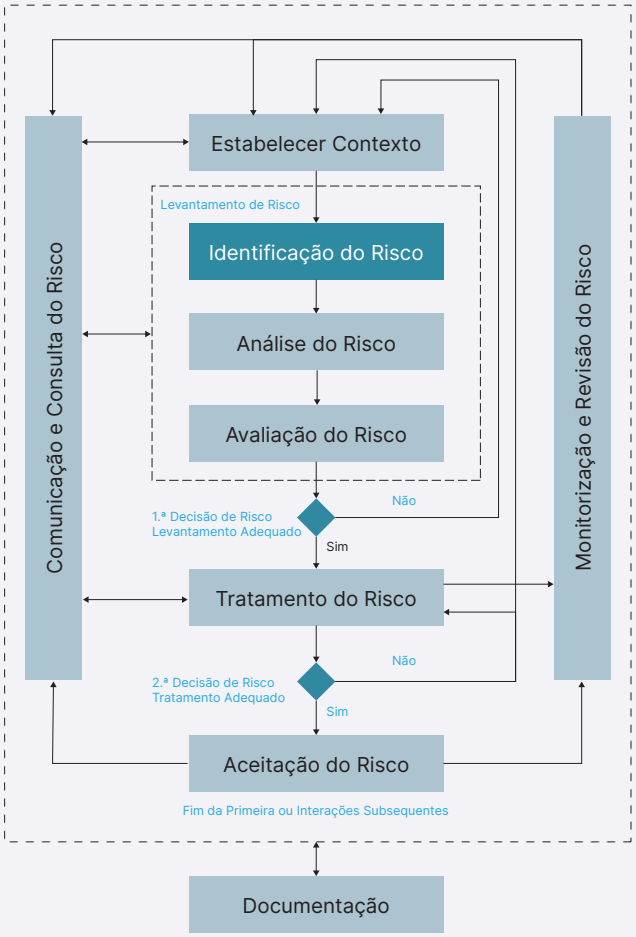

Figura 4 - "Identificação dos Riscos" - Processo de Gestão dos Riscos; Fonte: ISO/IEC 27005

É essencial que nesta etapa se incluam os riscos cujas fontes estão ou não, sob controlo da organização, mesmo que a fonte ou a causa dos riscos não seja evidente.

Para que a identificação dos riscos seja suficiente e adequada, a abordagem deve ser feita de forma metódica e organizada, a fim de garantir que todas as atividades relevantes são listadas e todos os riscos delas decorrentes tenham sido identificados.

As informações relevantes para a identificação dos riscos devem ser pertinentes e atualizadas, garantindo-se o envolvimento de recursos com o adequado conhecimento, e que são aplicadas técnicas de identificação dos riscos adequadas aos objetivos da organização, às suas capacidades e aos riscos enfrentados.

Para a identificação do risco podem ser realizadas várias atividades, como por exemplo:

- Análise de vulnerabilidades internas e externas;
- *Brainstorming* com os recursos envolvidos nos processos dentro do âmbito e fronteiras do processo de gestão dos riscos;
- Questionários com gestores ou responsáveis;
- Análise de cenários de ameaça internas e externas;
- Oficinas de avaliação dos riscos (*workshops*);
- Investigação de incidentes de cibersegurança;
- Auditorias de segurança;
- Comunicação com fornecedores, parceiros e clientes;
- Avaliações *(assessments)* dos riscos de segurança da informação e cibersegurança.

Sendo objetivo desta fase identificar, reconhecer e descrever os riscos que possam criar constrangimentos ou impedir a organização de atingir os seus objetivos, é necessário garantir a identificação dos ativos, ameaças, controlos existentes, vulnerabilidades e possíveis impactos.

A **Tabela 6** apresenta o exemplo de um processo a ser implementado na atividade de 'Identificação do Risco'.

Tabela 6 - Identificação dos Riscos

IDENTIFICAÇÃO DOS RISCOS		
Entradas (*Inputs*)	**Atividades**	**Saídas (*Outputs*)**
• *Feedback* de colaboradores e partes interessadas; • Análises de vulnerabilidades e/ou informações sobre incidentes de cibersegurança; • Taxonomias e outras fontes externas.	• Identificação e valorização de ativos; • Identificação de ameaças; • Identificação dos controlos existentes; • Identificação de vulnerabilidades; • Identificação das áreas impactadas/ consequências.	• Lista de ativos identificados; • Lista de ameaças; • Lista de controlos existentes; • Lista de vulnerabilidades; • Riscos devidamente identificados e documentados; • Lista de cenários plausíveis dos riscos.

A criação e disponibilização destas listas e catálogos deve ser realizada de forma transversal a todas as áreas envolvidas no processo de gestão dos riscos, devidamente enquadradas no âmbito estabelecido e enquadrado no contexto estabelecido.

As atividades descritas na **Tabela 6** sobre identificação dos riscos,auxiliam na recolha dos dados de entrada para as atividades de **Análise dos Riscos** (descrita no próximo subcapítulo).

Também nesta fase importa realçar alguns conceitos importantes:

- **Risco inerente:** O risco inerente é representado pela quantidade de risco existente sem qualquer tipo de controlos existentes associados.
- **Risco atual ou real:** O risco atual é representado pela quantidade de risco que existe com os controlos existentes no momento da identificação dos riscos.
- **Risco residual:** O risco residual é representado pela quantidade de risco que permanece ou que aparece após a inclusão dos controlos adicionais e/ou ajustes dos controlos já existentes.

a) Identificação e Valorização de Ativos

Um ativo é algo que tem valor para a organização e que, portanto, requer proteção na ótica da mesma.

No âmbito do RJSC, entende-se por "Ativo" "*todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos (aplicações e plataformas de software) considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços*".

No entanto, para o processo de gestão dos riscos de segurança da informação e cibersegurança, convém que se tenha em atenção que um sistema de informação compreende mais do que *hardware* e *software*, podendo os ativos ser (mas não só) das seguintes categorias:

- Tecnológicos (*hardware*, *software*, dispositivos de rede e sistemas);
- Pessoas;
- Informação;
- Ambiente Físico e Localizações;
- *Third* Party - consistem nas dependências contratuais internas ou externas ao serviço.
- (etc.).

O processo de análise dos riscos descrito no artigo 10.º do Decreto-Lei nº65/2021, de 30 de julho deve ser realizado para os ativos identificados no inventário de ativos (artigo 6.º), ou seja, os ativos essenciais para a prestação dos respetivos serviços. No entanto, para entidades que já possuem um maior grau de maturidade e que já contemplem e apliquem, de forma recorrente, processos de gestão dos risco, devem privilegiar uma análise mais holística e transversal, contemplando, também, as categorias de pessoas, localização, informação, etc.

O nível de detalhe recolhido e usado na identificação dos ativos influencia, diretamente, a quantidade geral de informação a ser trabalhada no processo de análise e avaliação dos riscos. Assim, a identificação dos ativos deve ser executada com o detalhe adequado, fornecendo informações suficientes para um processo de gestão dos riscos fidedigno.

A identificação ou inventariação de ativos não é um procedimento exclusivo do processo de gestão dos riscos, sendo uma atividade fundamental para a gestão e operacionalização de uma adequada estratégia de segurança da informação e cibersegurança.

Seja através de uma ferramenta, aplicação de gestão de ativos, ou de um catálogo de serviços informáticos aprovado, esta base de dados deve fornecer informação necessária para perceber a classificação do ativo de acordo com a sua criticidade para a organização, os processos da organização que são suportados por esse mesmo ativo e a identificação de dependências com outros ativos. Desta forma, é possível ter todos os ativos identificados, categorizados e listados, sendo recomendado que exista um inventário único.

A organização deverá ter procedimentos e práticas de atualização deste inventário, de forma a garantir que o mesmo está correto e atualizado, pois só assim será possível avaliar o potencial impacto, direto ou indireto, que algum risco terá na atividade da organização.

No inventário dos seus ativos, as entidades devem também identificar responsáveis para cada ativo, podendo equiparar-se ao "dono do risco", referido no capítulo anterior. O responsável pelo ativo pode não ter direitos de propriedade sobre este, mas tem responsabilidade sobre sua produção, desenvolvimento, manutenção, utilização e/ou segurança, conforme apropriado, sendo, frequentemente, a pessoa mais adequada para determinar o valor, interdependências e a criticidade do ativo para a organização.

Também as redes e sistemas de informação da organização que se encontram no exterior das suas instalações físicas devem ser identificados e catalogados no inventário de ativos; assim como a correta identificação das pessoas, dos ambientes físicos/localizações e as suas informações relevantes para a organização.

Note-se que o processo de gestão dos riscos também pode ser realizado também tendo por base o(s) processo(s) referentes à atividade da organização que os ativos suportam, tal como a ISO 9001 preconiza, fazendo-se associação a processo de negócio – ativo – risco.

Relativamente à criticidade, valorização ou classificação de cada um dos ativos, esta deve ser baseada no impacto decorrente de uma eventual falha ou indisponibilidade para a organização, e tem como objetivo garantir que os ativos recebem um nível apropriado de proteção, em função dessa sua importância. Esta classificação pode ter por base requisitos legais, valor, criticidade e a sensibilidade para o manuseamento da informação contida no ativo, entre outros.

A título de exemplo, a criticidade dos ativos pode ser determinada pelo valor de reposição do ativo, nomeadamente recuperação, limpeza ou substituição da informação. Outro exemplo de valorização dos ativos poderá ser em função dos valores de Confidencialidade, Integridade e Disponibilidade, através da aplicação do máximo dos valores referentes a estas dimensões:

Max (Confidencialidade; Integridade; Disponibilidade) = Valorização de ativo

A **Figura 5** apresenta alguns exemplos de níveis de classificação dos ativos:

Figura 5 - Níveis de classificação dos ativos

b) Identificação das Ameaças

Uma ameaça tem o potencial de poder criar impactos e consequências negativas nos ativos da organização (que podem ser informações, processos, sistemas, pessoas, etc.) e, consequentemente, comprometer as organizações.

As ameaças podem surgir de dentro ou de fora da organização, podendo ser de origem natural ou humana, e ser acidental ou intencional.

A experiência adquirida pela organização na gestão e aprendizagem de incidentes de cibersegurança e respetivas ameaças deve ser tida em consideração para a avaliação do risco atual.

A informação sobre possíveis ameaças pode ser obtida das seguintes formas:

- Revisão de incidentes de cibersegurança ocorridos;
- Auscultação do responsável pelo ativo;
- Perceção dos utilizadores;
- Pareceres de especialistas de segurança da informação, cibersegurança e segurança física;
- Informações dos departamentos legais;
- Informação veiculada através de meios de comunicação;
- Informação comunicada ou disponibilizada por instituições públicas e/ou outras com relevo para a segurança da organização ou nacional;
- Catálogo de ameaças comuns como as sugeridas no Anexo A deste documento; e
- Catálogo de ameaças do setor/área de atuação.

De acordo com artigo 10-º do Decreto-Lei nº65/2021, de 30 de julho a identificação das ameaças podem incluir nomeadamente as categorias de:

- Falha de sistema;
- Fenómeno natural;
- Erro humano;
- Ataque malicioso;
- Falha no fornecimento de bens ou serviços por terceiro.

Consulte o **Anexo A** do presente documento que contempla a identificação de ameaças segundo esta categorização.

c) Identificação dos Controlos Existentes

Na identificação dos vetores de risco, é necessário verificar a eficácia dos controlos implementados na organização, face ao cenário atual, para evitar custos e trabalhos desnecessários como, por exemplo, na duplicação de controlos. Através desta identificação passa a ser possível a identificação do risco real (até aqui teríamos um risco inerente), uma vez que é representado pela quantidade de risco que existe com os controlos existentes no momento da identificação dos riscos.

Os controlos podem ser processos, políticas, dispositivos, práticas ou outras ações que modifiquem o risco. Note-se que os controlos nem sempre exercem o efeito de modificação pretendido ou assumido.

São exemplos de controlos de segurança, as medidas de segurança documentadas no QNRSC, organizadas através dos objetivos de Identificar, Proteger, Detetar, Responder e Recuperar. Para a identificação dos controlos existentes, devem ser consideradas, a título de exemplo, as seguintes atividades:

- Revisão de documentos que contenham informações sobre a implementação dos controlos (por exemplo: planos anteriores de implementação de processos de gestão do risco). Se os processos de gestão da segurança da informação estiverem corretamente documentados, todos os controlos planeados e/ou existentes e o seu respetivo estado de implementação deverão estar disponíveis para consulta e análise;
- Verificação junto dos responsáveis pela segurança da informação e cibersegurança (por exemplo: CISO, COO) sobre quais são os controlos que se encontram efetivamente implementados;
- Realização de uma avaliação presencial, no local, para aferir a implementação dos controlos físicos, comparando os que estão devidamente implementados com a lista dos controlos que deveriam estar e, verificando entre os implementados, se estes se encontram correta e eficazmente operacionalizados.

Deve ter-se em consideração que um controlo ou conjunto de controlos que estejam incorretamente implementados, podem traduzir-se em potenciais vulnerabilidades para a organização, logo devem ser identificados controlos complementares e/ou ações de forma que esse controlo mesmo seja substituído ou removido para endereçar esses riscos de forma eficaz.

A avaliação da maturidade de cada controlo pode ser inspirada nos níveis de capacidade do **Quadro de Avaliação de Capacidades de Cibersegurança.** Este Quadro define três níveis de capacidade, como demonstrado na **Tabela 7**, o nível "1 – INICIAL", "2 – INTERMÉDIO" e "3 – AVANÇADO". Considera-se determinado nível de maturidade atingido quando todas as capacidades descritas no próprio nível e inferiores são cumpridas.

Tabela 7 - Níveis de capacidade para identificação dos controlos

NÍVEIS DE CAPACIDADE	DESCRIÇÃO
1 – INICIAL	Medidas de segurança básicas que poderiam ser implementadas para alcançar o objetivo de segurança, nomeadamente em iniciativas *ad-hoc,* por iniciativas isoladas e pouco formais.
2 – INTERMÉDIO	Medidas de segurança que atendem à maioria dos casos e necessidades para atingir os objetivos de segurança da informação. As medidas são atingidas formalmente.
3 – AVANÇADO	Medidas de segurança avançadas que envolvem a monitorização contínua dos controlos, avaliação e revisão recorrentes, levando em consideração alterações, incidentes, testes e exercícios, para melhoria proativa das mesmas.

d) Identificação das Vulnerabilidades

Uma vulnerabilidade é um ponto fraco de um ativo ou de um controlo que pode ser explorado por uma ameaça, sendo esta última, tal como já referido, uma potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização.

O ambiente da organização pode estar sujeito a uma grande variedade de vulnerabilidades, as quais podem ser identificadas nomeadamente através do uso de ferramentas próprias, como a realização de análises ou *scans* de vulnerabilidades e de *pentesting* (teste de intrusão em redes ou sistemas).

No entanto, e de forma mais abrangente, poderá encontrar no **Anexo B** deste documento um catálogo de vulnerabilidades, de forma a auxiliar a sua utilização no processo de gestão dos riscos e que são categorizadas a nível de:

- *Hardware*;
- *Software*;
- Rede;
- Pessoas;
- Local ou instalações; e
- Organização e seus processos e procedimentos.

A seguir, são apontados alguns exemplos de vulnerabilidades mais comuns:

- Uso inadequado ou negligente do controlo de acesso físico a edifícios e salas;
- Suscetibilidade de variações de corrente elétrica;
- Ponto único de falha;
- Procedimentos de teste de software insuficientes ou inexistentes;
- Inexistência de cópias de segurança (“backup”)
- Transferência de palavras-passe em claro;
- Falta de controlos para a gestão de ativos fora das instalações;
- Utilização incorreta de *software* e *hardware*;
- Falta de registos nos *logs* de administrador e operador;
- Manutenção insuficiente e/ou instalação defeituosa de suportes de armazenamento de dados, entre outros.

É importante referir, no entanto, que a existência de uma ou mais vulnerabilidades por si só não causa danos. Para que ocorra um dano é necessário que exista uma ameaça intencional ou não, que explore ou seja promovida por essa(s) vulnerabilidades.

Um processo de gestão dos riscos apto a atingir as finalidades para as quais foi criado deve derivar de um processo de gestão de vulnerabilidades eficiente e criterioso, pois a partir deste último é que os riscos poderão ser satisfatoriamente identificados.

ETAPA 2 - ANÁLISE DOS RISCOS

A segunda etapa do processo de levantamento dos riscos é a 'Análise dos Riscos'.

A **Análise dos Riscos** tem como objetivo verificar quais as origens dos riscos identificados, as suas consequências e impactos e qual a probabilidade da sua ocorrência.

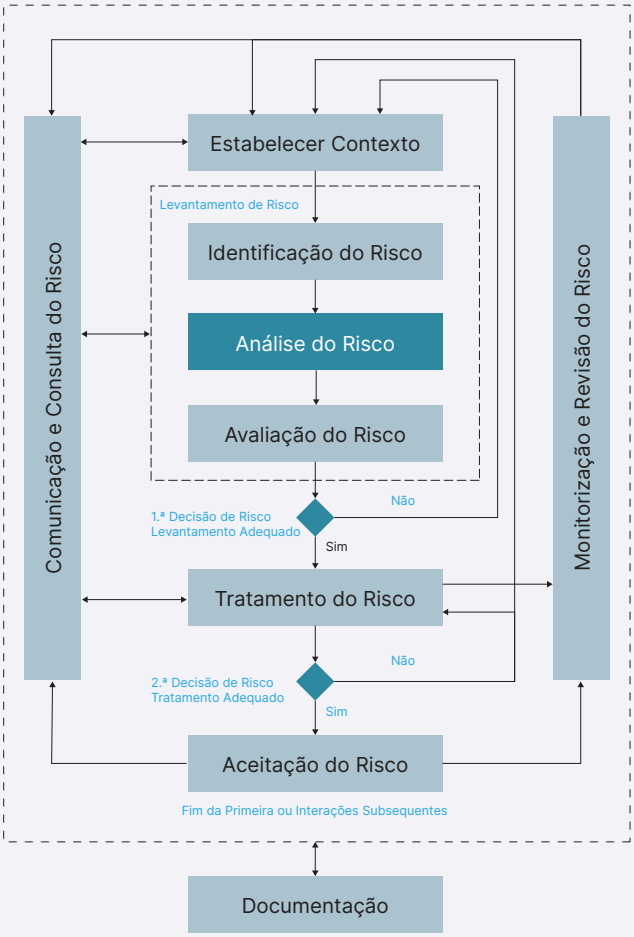

Figura 6 - "Análise dos Riscos" - Processo de Gestão dos Riscos; Fonte: ISO/IEC 27005

Para execução desta fase, a organização deverá dispor de uma lista com a identificação das ameaças e vulnerabilidades, dos ativos afetados, e dos controlos implementados e sua eficácia, que deverão ter resultado como saídas ou *outputs* da fase anterior (etapa 1 - Identificação dos Riscos).

O risco é expresso como a combinação do impacto de um evento e a sua probabilidade de acontecer.

Risco=Probabilidade x **Impacto**

Essa equação pode, no entanto, ser expandida para refletir a ameaça da exploração das vulnerabilidades nos ativos, substituindo-se o conceito de 'probabilidade' pela 'probabilidade da ameaça que explora a vulnerabilidade'. Adotando também o princípio de que o valor do 'impacto' é a consequência ou custo total de um ativo comprometido, pode reformular-se a equação do seguinte modo:

Risco=(probabilidade da ameaça explorar a vulnerabilidade)
***X* (custo total do impacto do ativo comprometido)**

De forma a determinar o risco é recomendada a utilização de **Matrizes de Risco** (será abordado no *capítulo c) sobre Determinação do nível de risco*), registando o valor do risco como o mais alto de todas as causas identificadas.

a) Metodologia de Análise dos Riscos

A metodologia de análise dos riscos pode ser abordada de forma analítica com caráter qualitativo, quantitativo ou por uma combinação de ambas.

- **Análise qualitativa do risco:** utiliza uma escala de atributos de qualificação para identificar a severidade dos potenciais impactos (por exemplo: Baixo, Médio e Alto) e a probabilidade de tais ocorrências. Uma das desvantagens desta metodologia é a subjetividade da escala em questão. As análises qualitativas deverão utilizar dados e informações factuais.

- **Análise quantitativa do risco:** utiliza uma escala de valores numéricos para aferição dos impactos e probabilidades, devendo suportar-se em diversas fontes. A qualidade da análise depende da exatidão e integridade dos valores numéricos e da validade dos modelos utilizados. A análise quantitativa dos riscos utiliza, na maioria dos casos, dados de históricos de incidentes, apresentando, assim, a vantagem de poder ser diretamente relacionada com os objetivos e preocupações de segurança da informação da organização. Por outro lado, a análise quantitativa poderá ser desvantajosa, caso não existam dados factuais e/ou auditáveis, criando uma ilusão de precisão e de eficácia do processo de avaliação do risco.

A metodologia de análise dos riscos a utilizar deverá ser consistente com o definido na fase de 'Estabelecer Contexto'.

Neste Guia irá optar-se por uma metodologia de análise dos riscos do tipo qualitativa, uma vez que este documento tem como público-alvo um conjunto muito diverso de organizações de diversos setores, dimensões e maturidade. Com isto, pretende-se facilitar a compreensão das várias partes interessadas no que concerne a indicadores gerais do nível do risco, permitindo a identificação dos riscos mais relevantes.

b) Critérios de Probabilidade e Impacto

Os critérios para a definição da probabilidade e do impacto dos riscos devem ter em consideração o contexto descrito anteriormente, os objetivos de negócio da organização, bem como os próprios objetivos do processo de gestão dos riscos. Essa análise deve ser feita de maneira criteriosa e consistente.

A probabilidade descreve a frequência expectável de acontecer o evento de risco num determinado período. Este valor pode ser baseado em informação estatística de incidentes já ocorridos e/ou na opinião de especialistas.

De acordo com artigo 10º do Decreto-Lei nº65/2021 de 30 de julho realização da Análise dos Risco deverá também ter em consideração:

- O histórico de situações extraordinárias ocorridas;
- O histórico de incidentes e, em especial, de incidentes com impacto relevante;
  - O número de utilizadores afetados pelos incidentes ocorridos;
  - A duração desses incidentes;
  - A sua distribuição geográfica, no que se refere à zona afetada;
  - As dependências intersectoriais para efeitos da prestação dos serviços.

Denote-se que a probabilidade não tem necessariamente uma relação diretamente proporcional ao impacto, podendo a probabilidade ser muito alta de acontecer e o impacto ser muito baixo.

As diretrizes para os critérios de análise dos riscos podem ser identificadas na **Figura 7**.

Critérios de Análise de Riscos		
Risco	**Probabilidade**	**Impacto**
Muito Alto [5]	Evento tem ocorrido frequentemente. Há registo de várias ocorrências e é provável que venha a ocorrer novamente num intervalo igual ou inferior a 1 ano.	Evento que gera impacto sobre toda a organização ou representa perda de disponibilidade, confidencialidade e/ou integridade causando prejuízos de forma generalizada, inviabilizando todas as funções primárias ou proporcionando percepção negativa
Alto [4]	Evento tem ocorrido frequentemente. Há registo de mais de uma ocorrência e é provável que venha a ocorrer novamente num intervalo de 1 ano.	Evento que gera impacto sobre vários grupos ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções primárias de trabalho de múltiplas áreas da organização.
Médio [3]	Evento tem ocorrido, porém não frequentemente. Há registos de uma ocorrência no intervalo de 1 ano.	Evento que gera impacto sobre um grupo relevante ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções primárias de trabalho.
Baixo [2]	Evento já ocorreu nesse tipo de atividade e é possível que venha a ocorrer novamente no intervalo de 1 ano ou supenor	Evento que gera impacto sobre um pequeno grupo ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funcões secundárias de trabalho, não sendo bastante para intervir nas funções principais.
Muito Baixo [1]	Evento nunca ocorreu nesse tipo de atividade e é altamente improvável que venha a ocorrer num intervalo superior a 3 anos.	Evento que gera impacto sobre apenas uma pessoa ou representa perda de disponibilidade, confidencialidade e/ou integridade que não necessita de intervencão ou paralisação imediata.

Figura 7 - Critérios de análise dos riscos

A fim de realizar uma melhor aferição do impacto do risco, a organização pode, por outro lado, identificar o impacto analisando potenciais consequências operacionais. Podem ser utilizadas as seguintes categorizações:

- **Legal/regulatório** – qualquer consequência que a organização possa sofrer a nível legal e/ou regulatório a nível nacional e internacional, como por exemplo, decorrente do RJSC ou do Regulamento Geral sobre a Proteção de Dados;
- **Perdas operacionais/financeiras** – área que pesa a perda de capacidades da operacionalidade dos serviços prestados, nomeadamente dos serviços TIC e do SGSI, assim como a perda financeira inevitável forma fim de recuperar a capacidade anterior à materialização do risco;
- **Perdas de produtividade** – área que pondera o impacto causado ao nível interno na prestação do serviço, bem ou do sistema, que force os colaboradores ou partes interessadas a não cumprir com as suas funções e responsabilidades;
- **Perdas de clientes** – avalia o impacto que o risco possui na carteira de clientes e/ou parceiros da organização;
- **Reputação e imagem** – área focada no impacto obtido pela materialização do risco para a imagem e reputação que a organização possui externamente, como, por exemplo, a perda da confiança das partes interessadas;
- **Segurança e saúde** – área que reflete o impacto da materialização dos riscos a nível de saúde e segurança pessoal que deve ser garantida a colaboradores e partes interessadas da organização.

A **Tabela 8 - Definição de cada nível de impacto para todas as áreas de consequências aquando da materialização dos riscos** apresenta uma caracterização de cada nível de impacto operacional para todas as áreas de avaliação, aquando da materialização dos riscos.

Tabela 8 - Definição de cada nível de impacto para todas as áreas de consequências aquando da materialização dos riscos

Níveis de impacto	Legais e Regulatórios	Perdas Operacionais/ Financeiras	Perdas de Produtividade	Perdas de Clientes	Reputação e Imagem	Segurança e Saúde
Muito Alto (5)	Impacto legal/ regulatório muito alto, com coimas altas associadas, podendo interromper a prestação do serviço, bem ou sistema	Quebra operacional significativa, podendo ser total e/ou definitiva	Impacto interno e externo comprometendo a prestação do serviço, bem ou sistema forçando os colaboradores ou partes interessadas a não cumprir com as suas funções e responsabilidades	Descontentamento generalizado de um grupo de clientes críticos ao negócio, sem possibilidade de reverter a situação	Evento é conhecido externamente à organização e foi publicado por fontes de comunicação social, incluindo internacionalmente	Com registo de ausência colaboradores com baixa médica ou de seguro, com impacto total na organização
Alto (4)	Impacto legal/ regulatório de alto impacto com coimas associadas	Quebra operacional parcial com impacto elevado nas operações	Impacto interno ou externo comprometendo a prestação do serviço, bem ou sistema forçando os colaboradores ou partes interessadas a não cumprir com as suas funções e responsabilidades	Descontentamento de um grupo de clientes críticos ao negócio com possibilidade de reverter a situação.	Evento é conhecido externamente à organização e foi publicado por pessoas individuais	Com registo de ausência colaboradores com baixa médica ou de seguro, com impacto em mais do que um departamento da organização
Médio (3)	Impacto legal/ regulatório de médio impacto	Quebra operacional parcial com algum impacto residual nas operações	Impacto interno ou externo comprometendo a prestação do serviço, bem ou sistema forçando os colaboradores ou partes interessadas a não cumprir parcialmente com as suas funções e responsabilidades	Descontentamento de um grupo de clientes considerável com possibilidade de reverter a situação.	Evento ficou circunscrito internamente na organização	Com registo de ausência colaboradores com baixa médica ou de seguro, com impacto num departamento ou área da organização
Baixo (2)	Impacto legal/ regulatório de baixo impacto	Quebra operacional parcial com muito baixo impacto nas operações	Impacto interno comprometendo a prestação do serviço, bem ou sistema, porém não interrompendo os colaboradores a cumprir com suas funções e responsabilidades	Descontentamento de um grupo reduzido de clientes com possibilidade de reverter a situação.	Evento ficou circunscrito internamente no departamento ou área afetada	Com registo de ausência colaboradores com baixa médica ou de seguro, sem impacto nas funções da organização
Muito Baixo (1)	Sem impactos previstos ao nível legal/regulatório	Sem impacto operacional / Financeiro para a organização	Impacto interno não comprometendo a prestação do serviço ou sistema, e não interrompendo os colaboradores a cumprir com suas funções e responsabilidades	Descontentamento de um grupo pequeno de clientes com possibilidade de reverter a situação no imediato.	Evento ficou circunscrito internamente na área afetada	Sem registo de ausência colaboradores com baixa médica ou de seguro

Observações: As descrições na tabela acima são sugestivas, podendo ser alteradas de acordo com os critérios que forem mais convenientes para a organização.

Cabe à organização selecionar se pretende fazer uma análise de impacto tendo em consideração um critério genérico ou através de uma categorização a nível operacional. No caso de existirem várias áreas de consequência com níveis de impacto distintos, o nível de impacto a considerar deverá ser o nível que apresente valor mais elevado.

c) Determinação do Nível de Risco

Tal como já referido, o risco é obtido através da relação de um potencial impacto ao negócio e a probabilidade de materialização dos riscos.

O nível do risco poderá ser designado numa escala de:
- **5** – muito alto;
- **4** – alto;
- **3** – médio;
- **2** – baixo;
- **1** – muito baixo.

Esta definição possibilita que se estabeleça uma ordem de priorização para o tratamento dos riscos críticos, de acordo com o nível que receberem.

A escala do nível de risco é definida da seguinte forma:

- **20 a 25** – muito alto;
- **12 a 19** – alto;
- **5 a 11** – médio;
- **2 a 4** – baixo;
- **1** – muito baixo.

A **Matriz de Riscos** na **Figura 8** distribui os riscos da seguinte maneira:

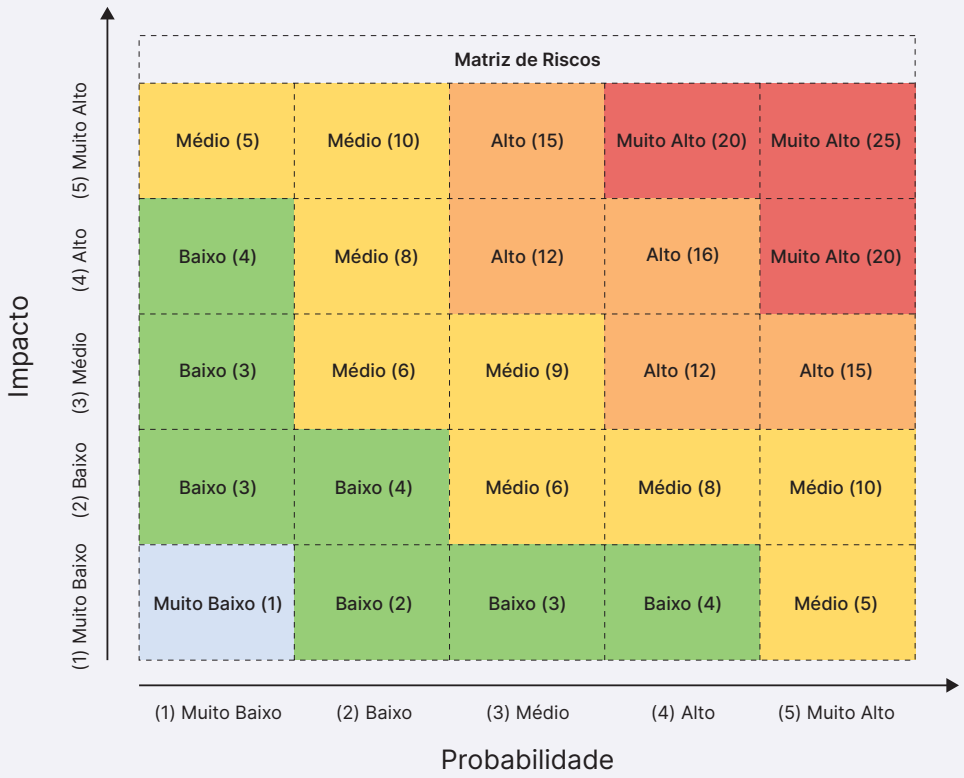

Figura 8 - Matriz de riscos

Existem eventos que têm consequências e impactos graves no negócio de uma organização e, aparentemente, uma muito baixa probabilidade de ocorrer. Esse tipo de evento é vulgarmente chamado de Cisne Negro, dado que descreve acontecimentos altamente improváveis. Podemos exemplificar este tipo de eventos com o Ataque das Torres Gêmeas em 11 de setembro (2001), o Acidente Nuclear de *Fukushima* (2011), ou até mesmo o efeito da pandemia COVID-19 (2020).

Apesar de difícil perspetivar uma situação destas, este tipo de eventos também deve ser considerado num processo de gestão dos riscos.

d) Definição do Nível de Risco para Serviços Essenciais

Os Operadores de Serviços Essenciais (OES) são organizações públicas ou privadas que prestam um serviço essencial, enquadrando-se num dos tipos de entidades que atuam nos setores e subsetores constantes do anexo ao RJSC, e que são identificados pelo Centro Nacional de Cibersegurança

Atendendo à própria definição de OES, acredita-se que uma falha ou interrupção de um serviço essencial terá um impacto significativo na sociedade, pelo que se propõe a utilização de uma Matriz de Riscos mais conservadora como a apresentada na **Figura 9**.

Nesta matriz, deve ter-se em atenção que o impacto da materialização do risco deve ter um peso maior do que a probabilidade da sua ocorrência.

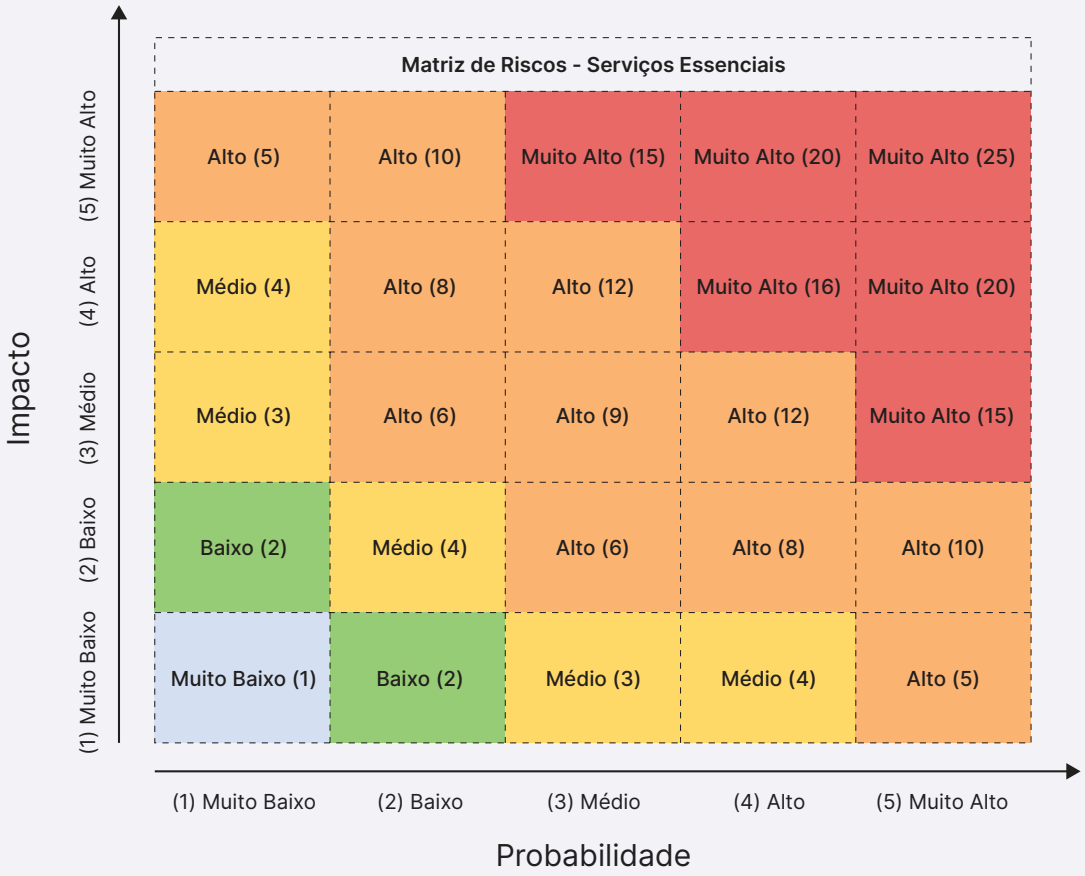

Figura 9 - Matriz de risco para os operadores de serviços essenciais

Finalizada esta etapa da análise dos riscos, é assignado a cada cenário identificado um valor ao impacto e probabilidade de ocorrência.

ETAPA 3 - AVALIAÇÃO DOS RISCOS

A terceira e última etapa do processo de levantamento dos riscos é a 'Avaliação dos Riscos'.

A etapa **Avaliação dos Riscos** tem a finalidade de auxiliar na tomada de decisão sobre o tratamento dos riscos, baseando-se principalmente na premissa de um nível aceitável dos riscos.

Com base na identificação e análise do nível dos riscos realizados nas etapas anteriores, devem ser avaliados quais os riscos que necessitam de tratamento para serem mitigados, transferidos ou evitados e quais os que podem ser aceites dentro do contexto da organização e/ou que se encontram devidamente enquadrados no nível de aceitação do risco estabelecido no início.

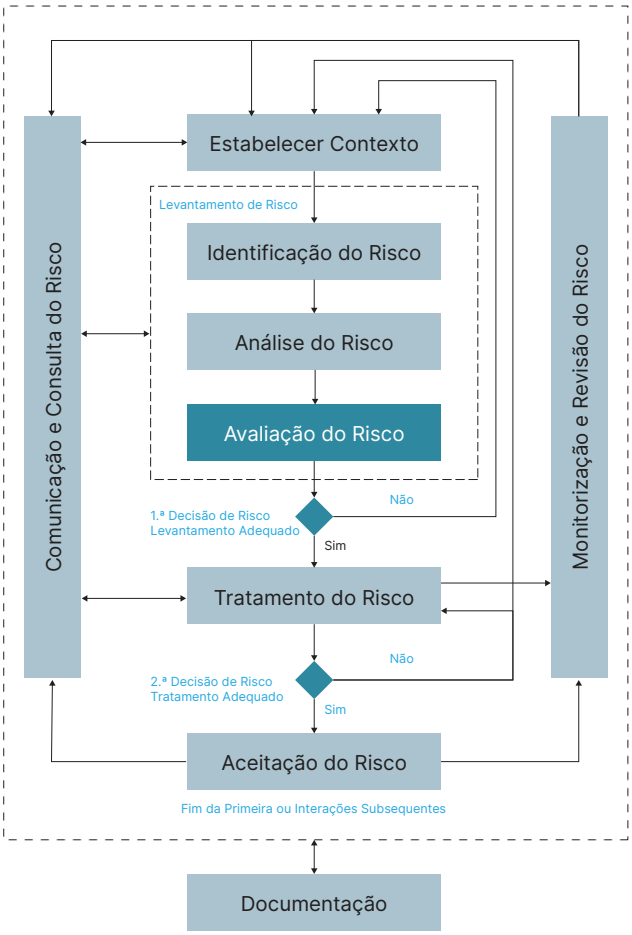

Figura 10 - "Avaliação dos Riscos" - Processo de Gestão dos Riscos; Fonte: ISO/IEC 27005

Esta fase da avaliação dos riscos permite uma deliberação consciente sobre quais os tratamentos que devem ser usados e por que ordem de priorização os riscos devem ser tratados. É importante considerar que tais decisões, para que sejam tomadas adequadamente, não podem desconsiderar os requisitos legais, normativos e regulatórios e outros pressupostos aos quais a organização esteja sujeita.

Alguns critérios utilizados para avaliação dos riscos de segurança da informação e cibersegurança são:

a) Avaliação das Consequências no Negócio

Neste passo é onde se fará a avaliação propriamente dita dos cenários de eventos identificados como relevantes para as atividades da empresa, tendo em consideração a identificação dos ativos de informação envolvidos, ameaças, controlos existentes, vulnerabilidades, e consequências para os ativos (através da identificação de impacto e probabilidade de ocorrência) e processos de negócio, visando identificar e medir o potencial impacto sobre a organização.

Se um critério não é relevante para a organização como por exemplo a perda da confidencialidade, dado que só trabalha com dados públicos, então todos os riscos que impactam este critério podem não ser relevantes.

b) Limites de Aceitação do Risco

Tendo a organização definido os critérios de aceitação do risco, deverá identificar a partir de que nível de risco terá que ser necessária a aprovação formal da gestão de topo para que o mesmo possa ser aceite.

Por outro lado, os critérios de aceitação podem diferir de acordo com o seu tempo de vida do risco, caso este esteja associado a uma atividade temporária ou de curto prazo da organização.

c) Priorização de Acordo com o Nível de Risco e a Relevância para o Negócio

Nesta fase, conforme mencionado anteriormente, cada organização deverá estabelecer uma ordem de prioridade para o risco, de acordo com uma análise detalhada entre o nível dos riscos e as proporções das suas consequências para a organização dentro das suas particularidades, como ramo de atividade, organização interna, objetivos de negócio etc.

Se o processo ou ativo tiver sido definido de baixa importância, convém que os riscos associados a ele sejam menos relevantes do que os riscos que causam impactos em processos, atividades ou ativos mais importantes ou até essenciais para o fornecimento de bens ou prestação de serviços.

V. TRATAMENTO DOS RISCOS

A fase de **Tratamento dos Riscos** envolve a identificação, formalização e implementação de um ou mais planos de ação, os quais têm como objetivo controlar e/ou mitigar as causas do risco identificadas na fase de levantamento dos riscos.

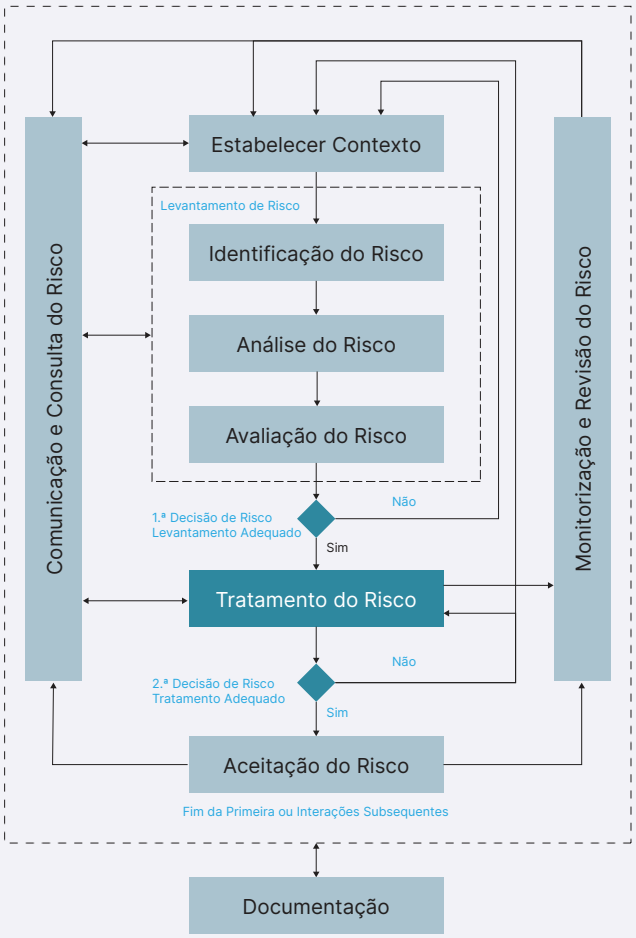

Figura 11 - "Tratamento do risco" - Processo de Gestão dos Riscos; Fonte: ISO/IEC 27005

Neste âmbito, é imprescindível que seja definido um responsável e uma data para a implementação dos planos e correspondentes ações de tratamento. O objetivo é que, uma vez concluídos os planos de ação estes reduzam, em consequência, o nível de risco.

Os possíveis tratamentos aos riscos estão descritos a seguir:

- **Mitigar ou Modificar:** Diminuir a exposição dos riscos, elaborando planos de ação e aplicando controlos específicos, podendo haver lugar à implementação de controlos adicionais de forma a mitigar o risco ou reduzi-lo de modo a enquadrar-se nos critérios de aceitação dos riscos definidos pela organização.
- **Evitar:** Eliminar a causa do risco, eliminando o processo que o gera. Visa a descontinuação das atividades de negócio ou ativos de informação ou de suporte que atuam como fonte do risco para a organização, eliminando de forma permanente o risco. Tipicamente esta opção é considerada quando o plano de tratamento apresenta custos demasiado elevados e que a atividade de negócio ou ativo visadas já não possua uma importância tão visível para os objetivos de negócio da organização.
- **Transferir ou Partilhar:** Direcionar a responsabilidade das consequências a terceiros. A responsabilidade pelo risco é transferida para outra entidade que não a organização, como por exemplo, assegurar os ativos ou atividades de negócio através da atribuição da responsabilidade destes a fornecedores ou outros parceiros.
- **Aceitar ou Retenção:** Tomar conhecimento do risco sem adotar controlos. Neste caso é suportada a decisão de não aplicar qualquer tipo de ação corretiva ao risco e assumir as consequências que o mesmo pode trazer à organização em caso de materialização. Somente riscos de nível baixo e muito baixo devem ser retidos. Esta opção deve ser utilizada em situações em que:
  - O risco se encontra dentro dos critérios de aceitação definidos pela organização;
  - Quando a implementação dos controlos para a redução do nível apresenta custos superiores àqueles que o risco provoca em caso de materialização.

A **Tabela 9** apresenta um exemplo do tratamento recomendado para cada valor de risco identificado:

Tabela 9 - Exemplo de Tratamento dos Riscos

Valor do Risco e respetivo Tratamento	
Descrição	**Tratamento recomendado**
Muito Baixo	Aceitar
Baixo	Aceitar/Mitigar/Transferir
Médio	Mitigar/Transferir
Alto	Mitigar/Transferir
Muito Alto	Evitar

O departamento responsável pela análise, avaliação e tratamento dos riscos identificados deve ainda ter como responsabilidade a avaliação e elaboração dos planos de tratamento dos riscos, de acordo com o processo de tratamento ilustrado na **Figura 12.**

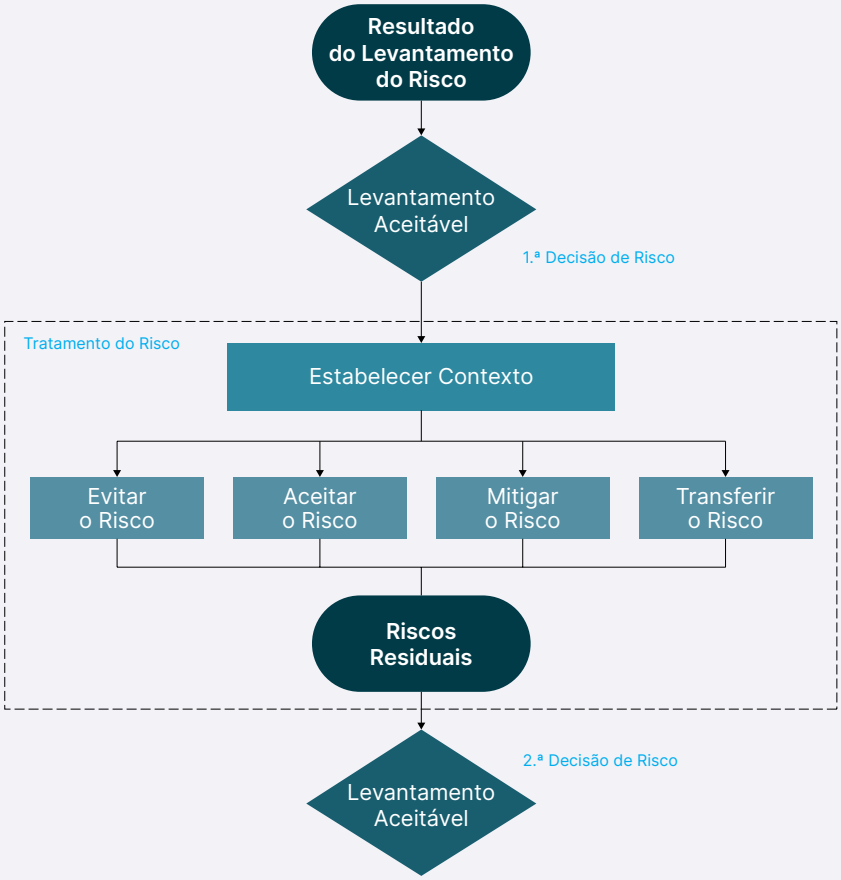

Figura 12 - Tratamento dos Riscos; Fonte: ISO/IEC 27005

O tratamento dos riscos é um processo cíclico, composto por várias fases, as quais, em linhas gerais, consistem em:

- Avaliar o tratamento dos riscos que já foi realizado pela organização;
- Analisar e decidir se os níveis de risco residual são toleráveis para a organização;
  - Em caso negativo, definir e implementar um novo tratamento para os riscos em questão;
- Avaliar a eficácia dos tratamentos recém implementados.

As opções para o tratamento dos riscos são diversas e podem ser implementadas de forma individual ou simultânea. A seleção das opções mais adequadas para cada caso deve ter em conta o nível dos riscos em questão, os custos e esforços para a implementação do tratamento escolhido e, ainda, os benefícios desse tratamento para a organização ou, segundo a mesma perspetiva, os prejuízos que tal tratamento estará a evitar ou prevenir.

Os riscos identificados como "Muito Altos" devem ser, obrigatoriamente, tratados nomeadamente através de medidas de mitigação.

Atendendo à importância e imprescindibilidade de serviços prestados por Operadores de Serviços Essenciais para a economia e sociedade, estes devem tratar todos os riscos classificados como "Alto" e "Muito Alto".

Os planos de tratamento dos riscos servem para documentar quais as opções de tratamento que foram selecionadas, de que maneira e em que ordem deverão ser implementadas. Estes devem indicar os detalhes do procedimento de escolha e implementação dos tratamentos, como, por exemplo:

- as razões das referidas escolhas e os benefícios que se pretende alcançar através delas;
- identificar os responsáveis pela aprovação e pela implementação do plano de tratamento;
- identificar as ações que foram propostas;
- identificar os recursos, medidas de desempenho e restrições que são requeridos;
- apresentar um cronograma e o planeamento da implementação.

Os planos de tratamento dos riscos ainda devem indicar, de forma direta, a ordem de prioridade na implementação dos tratamentos que foram considerados necessários.

Os planos de tratamento dos riscos de segurança da informação e cibersegurança devem ser endereçados numa ferramenta ou sistema, para o correto acompanhamento e tratamentos dos riscos identificados.

A **Tabela 10** apresenta o exemplo de um processo a ser implementado na atividade de 'Tratamento dos Riscos', sendo que, após seguidos os passos apresentados, o ciclo de avaliação e implementação de tratamento dos riscos recomeça.

Tabela 10 - Tratamento dos riscos

TRATAMENTO DO RISCOS		
Entradas (*Inputs*)	**Atividades**	**Saídas (*Outputs*)**
Riscos analisados	• Desenvolvimento de opções de tratamento dos riscos; • Planificação de tratamentos dos riscos; • Seleção de opções de tratamento; • Implementação de tratamentos dos riscos; • Análise da eficiência e eficácia dos tratamentos realizados; • Monitorização e revisão dos controlos implementados de acordo com os planos de tratamento dos riscos.	• Opções de tratamento; • Planos de tratamento dos riscos.

VI. COMUNICAÇÃO E CONSULTA DOS RISCOS

A **Comunicação e Consulta dos Riscos** é uma atividade que tem como objetivo alcançar não só o consenso sobre como gerir os riscos de segurança da informação e cibersegurança, através da troca e/ou partilha das informações sobre os riscos entre os responsáveis e as outras partes interessadas, como promover a consciencialização sobre a importância do processo de gestão dos riscos em toda a organização. Esta é uma atividade que deve ser realizada de forma contínua.

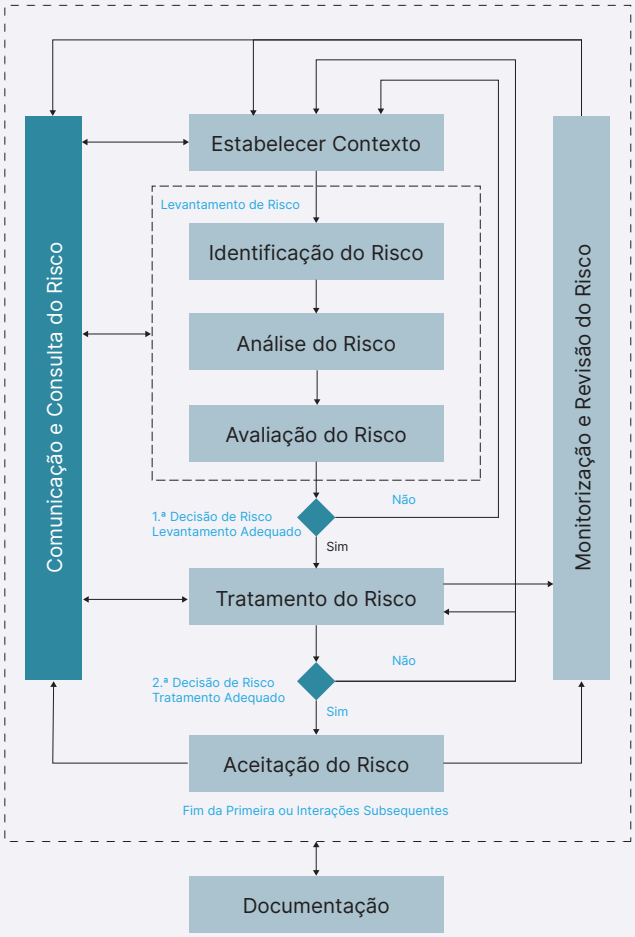

Figura 13 - "Comunicação e Consulta dos Riscos" -Processo de Gestão do Risco; Fonte: ISO/IEC 27005

É especialmente importante garantir que as perceções de risco das várias partes interessadas estão alinhadas, bem como suas perceções de benefícios, de forma que as ações específicas necessárias sejam claramente compreendidas e as decisões devidamente tomadas.

A coordenação entre os decisores, responsáveis e as partes interessadas pode ser alcançada pela constituição de um comité para promover a discussão sobre riscos, sua priorização e tratamento adequado, incluindo a sua aceitação. A realização periódica da revisão dos riscos e verificação do estado dos planos de tratamento dos riscos de segurança da informação e de cibersegurança, com apresentações e análise dos resultados à gestão de topo deve ser conside-

rada, principalmente para suportar as tomadas de decisão e demonstração de responsabilidade sobre os riscos.

É ainda fundamental compreender que sem a implementação de uma cultura de gestão dos riscos na organização, os objetivos e a segurança que se pretendem atingir poderão ser comprometidos, devendo ser dada a conhecer a estratégia e/ou política de gestão dos riscos da organização. Também a articulação e cooperação com outras unidades como departamentos de comunicação e relações externas é crucial, principalmente em casos de crises ou preparação de informações em resposta a incidentes específicos.

Recomenda-se que a organização estabeleça um plano e práticas de comunicação e consulta do risco para assegurar o compromisso dos responsáveis, internos ou externos, pelos riscos, de acordo com a estrutura do plano de comunicação criado. O plano de comunicação e consulta do risco deve assegurar que:

- Todos os outputs das práticas da gestão do risco, incluindo decisões de modificação dos mesmos, são comunicados via canais já definidos (incluindo acordos entre as partes sobre como gerir cada uma das práticas utilizadas no processo, como, por exemplo, o tratamento e resposta ao risco);
- A informação partilhada possui um nível de detalhe apropriado para atingir os objetivos do processo de gestão do risco e da organização;
- O conteúdo de informação reportada é derivado de decisões referentes ao processo de gestão dos riscos da organização e enviado para os responsáveis de risco acordados;
- As partes externas são informadas adequadamente sobre as decisões relacionadas com o processo de gestão do risco da organização sempre que aplicável;
- Os canais de comunicação são usados como um meio para conferir mais confiança e consciencialização das partes externas em relação à temática do risco e decisões decorrentes do processo de gestão do risco da organização.

Na **Tabela 11** é possível identificar as atividades relativas à comunicação e consulta do risco.

Tabela 11 - Comunicação e consulta

COMUNICAÇÃO E CONSULTA DOS RISCOS		
Entradas (*Inputs*)	**Atividades**	**Saídas (*Outputs*)**
Visões das partes interessadas relevantes	Elaboração do plano de comunicação e consulta	Plano de comunicação e consulta

VII. MONITORIZAÇÃO E REVISÃO DOS RISCOS

A organização tem a responsabilidade de monitorizar, com regularidade, o ecossistema da organização sobre a perspetiva do risco de segurança da informação e cibersegurança, não só porque os riscos não são estáticos, ou seja, as ameaças, vulnerabilidades, probabilidades e suas consequências estão sempre a alterar, como qualquer alteração significativa que possa existir no contexto interno e externo da organização, pode traduzir-se numa alteração à perceção do risco. Tal como a fase de "Comunicação e Consulta dos Riscos", também a monitorização e revisão dos riscos é realizada de forma contínua no processo de gestão dos riscos.

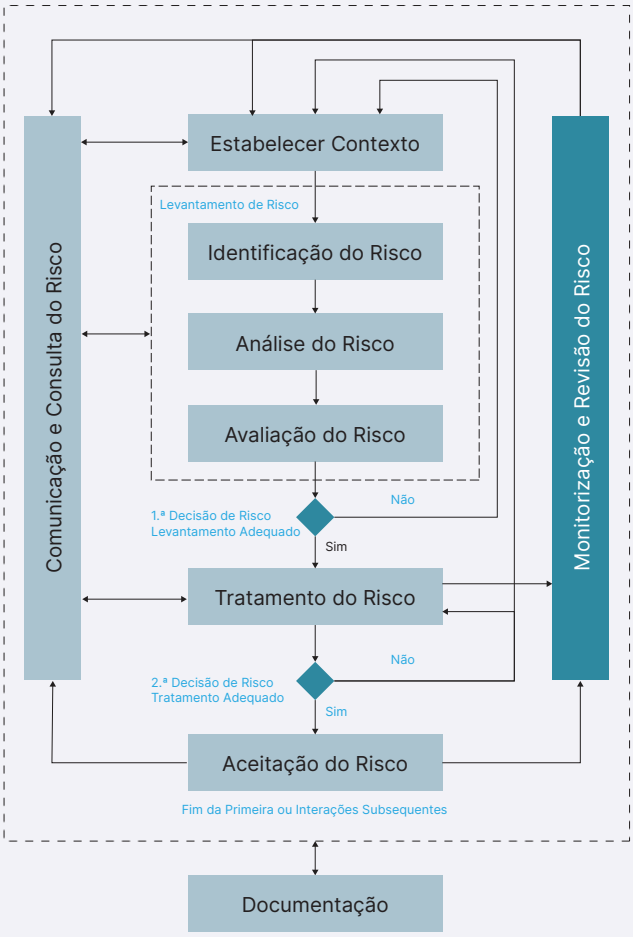

Figura 14 – "Monitorização e Revisão dos Riscos" - Processo de Gestão dos Riscos; Fonte: ISO/IEC 27005

A monitorização e a análise crítica dos riscos têm como finalidade:

- verificar a eficácia e a eficiência dos controlos implementados;
- obter informações adicionais para melhoria do processo de avaliação dos riscos como um todo;
- analisar eventos e possíveis incidentes, para que seja possível aprender com eles e minimizar probabilidade de ocorrência futura;
- identificar mudanças circunstanciais que podem modificar a classificação de nível do risco ou o tipo de tratamento que melhor se adequa aos objetivos de negócio;
- identificar os riscos emergentes.

É recomendável que os resultados obtidos em todas as fases do processo de gestão dos riscos sejam registados, para que seja possível estudar e aperfeiçoá-los contínua e progressivamente, além de auxiliar na análise de desempenho dos procedimentos, métodos e ferramentas já implementados.

A monitorização e a revisão contínua são também necessárias para garantir que o contexto, o resultado da avaliação e tratamento dos riscos, bem como planos de gestão, permanecem relevantes e apropriados para as circunstâncias.

Assim, a organização deve garantir que os seguintes pontos são monitorizados de forma contínua e contemplados no processo de gestão dos riscos interno:

- novos ativos para que sejam incluídos no âmbito do processo de gestão do risco;
- alterações na criticidade dos ativos para a organização (por exemplo: devido à alteração de requisitos de negócios);
- novas ameaças que podem estar ativas, tanto dentro como fora da organização, e que ainda não foram avaliadas;
- possibilidade de novas vulnerabilidades serem exploradas por ameaças;
- possível aumento do impacto, consequências das ameaças, vulnerabilidades ou dos riscos agrupados que resultem num nível inaceitável do risco;
- incidentes de segurança da informação que já ocorreram ou que possam ocorrer.

VIII. DOCUMENTAÇÃO E REGISTO DOS PROCESSOS E RESULTADOS

As organizações devem ter documentados os processos identificados nos capítulos anteriores, destacando-se os processos de levantamento dos riscos e de tratamento dos riscos.

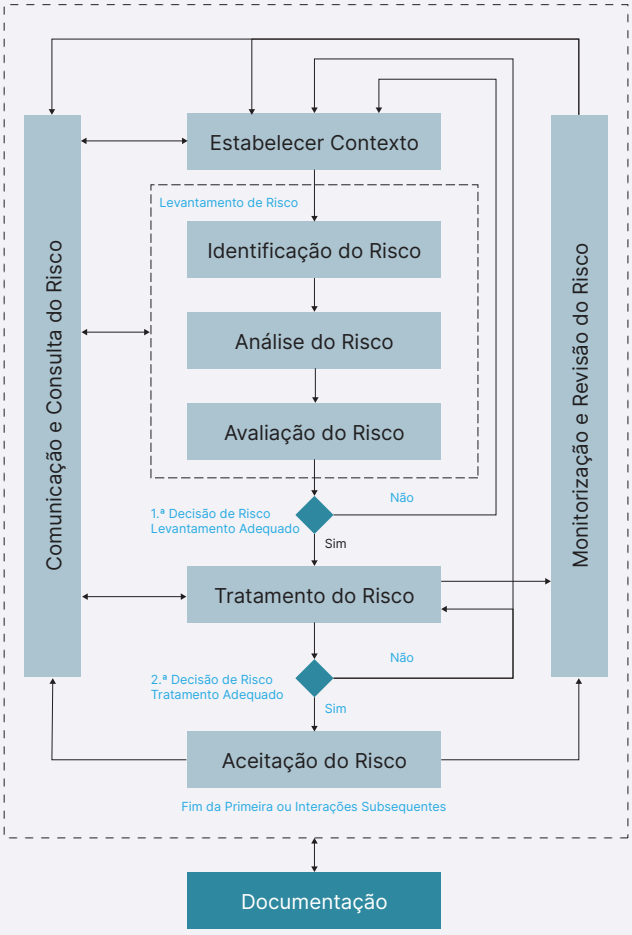

Figura 15 - "Documentação" - Processo de Gestão dos Riscos; Fonte: ISO/IEC 27005

Esta informação é importante pois serve de evidência a partes interessadas (por exemplo organismos de supervisão ou certificação) em como a organização leva a cabo um processo de gestão de risco, podendo também verificar a sua eficácia.

A título sugestivo, recomenda-se que sejam documentadas as seguintes informações associadas ao processo de levantamento:

- Definição dos critérios de risco (incluindo os critérios de aceitação de risco e os critérios para realizar avaliações de risco);
- Fundamentação da consistência, validade e comparabilidade dos resultados;
- Descrição do método de identificação do risco (incluindo a identificação dos donos do risco);
- Descrição do método de análise dos riscos (incluindo a avaliação de possíveis impactos e consequências, probabilidade realista e nível de risco resultante);
- Descrição do método de comparação dos resultados com os critérios de risco e a priorização dos riscos para tratamento de riscos.

No que concerne ao processo de tratamento dos riscos devem ser documentadas informações como:

- Método para selecionar opções apropriadas de tratamento dos riscos;
- Método para determinar os controlos necessários;
- Como são elaborados os planos de tratamento dos riscos;
- Como é obtida a aprovação dos donos do risco.

Todos os resultados decorrentes da aplicação e implementação dos processos de gestão dos riscos na organização devem também ser documentados e mantidos ao longo do tempo, pois facilitam não só a identificação de medidas de melhoria, tais como a necessidade de alteração de critérios de aceitação do risco, como permitem implementar processos mais eficazes de melhoria contínua.

Além disso, os resultados documentados permitem servir de evidência ao cumprimento de requisitos legais, uma vez que, no âmbito do Regime Jurídico da Segurança do Ciberespaço, as entidades abrangidas são obrigadas a realizar análise dos riscos em intervalos planeados ou quando mudanças significativas são propostas ou ocorrem.

Por último, a documentação da informação permite à organização ter um histórico fundamentado das decisões tomadas ao longo do tempo e que poderão ser relevantes em diversas situações. Destaque-se, no entanto, que a comparabilidade de diferentes resultados deve ter por base processos similares de gestão dos riscos.

IX. EXEMPLO

O João, responsável do Gabinete de Gestão de Projeto da Organização, identificou a necessidade da realização da análise dos riscos de forma a dar cumprimento ao artigo 10.º do Decreto-Lei n.º 65/2021, uma vez que a sua entidade se trata de um operador de serviço essencial.

Seguindo o descrito no presente Guia, o João deve iniciar a gestão dos riscos através do estabelecimento do contexto, onde identifica as funções e responsabilidades das partes interessadas no processo, como por exemplo determinando a matriz RACI para cada uma delas, os critérios de aceitação dos riscos e definição de âmbito e fronteiras, entre outras, conforme o exemplo abaixo.

Tabela 12 - Exemplo Matriz RACI

MATRIZ RACI - EXEMPLO			
Atividades	**Gestão de Topo**	**Gestor do Risco (João)**	**Dono do Risco**
Identificação dos riscos	I	R, A	R, C
Avaliação dos riscos	I	A	R
Análise dos Risco	R	C	I

Tabela 13 - Exemplo de Critérios de Aceitação dos Riscos

CRITÉRIOS DE ACEITAÇÃO DOS RISCOS - EXEMPLO		
Nível de Risco	**Critério de Aceitação dos Riscos**	**Priorização**
Muito alto	Não aceitável, requer tratamento imediato	1
Alto	Não aceitável, requer tratamento no prazo máximo de 15 dias	2
Médio	Não aceitável, requer tratamento no prazo máximo de 6 meses	3
Baixo	Risco cuja aceitação depende da avaliação do dono do risco, por norma será aceite, no entanto, pode decidir tratar.	4
Muito baixo	Risco aceitável, deve ser monitorizado e revisto a cada 12 meses.	5

Uma vez que o contexto está estabelecido, o João deve realizar o processo de levantamento dos riscos onde deve ter em conta as seguintes etapas:

Etapa 1 - Identificação dos riscos;

Para a identificação dos riscos, o João decidiu realizar uma avaliação dos riscos de segurança da informação e cibersegurança, onde fez a identificação de ativos, ameaças, controlos existentes e vulnerabilidades. Nesse sentido foi identificado os seguintes riscos:

Tabela 14 - Exemplo da Identificação dos Riscos

IDENTIFICAÇÃO DOS RISCOS - EXEMPLO					
Descrição	**Ativo**	**Ameaça**	**Controlos Atuais**	**Vulnerabilidade**	**Impacto genérico**
Indisponibilidade da plataforma devido a um ataque do tipo DDoS *Distributed Denial of Service*	Plataforma de Serviços para o Cliente.	Agente malicioso ou *botnet*	Níveis de proteção assegurados pelo prestador de serviços (Controlos Anti-DDoS)	• Conexões de rede pública não protegidas. • Resposta inadequada do serviço de manutenção.	Crítico para a entidade, em especial para os clientes que utilizam a plataforma.
Mau funcionamento da plataforma devido a especificações pouco claras ou incompletas.	Plataforma de Serviços para o Cliente.	Mau funcionamento de software	Processo de pedidos realizado e Ativos formalizado em memorando para alterações de maior complexidade.	Especificações para developers pouco claras ou incompletas	Crítico para a entidade, em especial para os clientes que utilizam a plataforma.
Indisponibilidade da plataforma devido a falhas no processo de gestão de vulnerabilidades.	Plataforma de Serviços para o Cliente.	Utilização não autorizada de equipamentos/ sistemas	Não existem controlos	Falta de procedimentos de reporte de vulnerabilidades de Segurança da Informação	Alta probabilidade tendo em conta o número de vulnerabilidades detetadas diariamente, e o facto da plataforma estar acessível na Internet.

Etapa 2 - Análise dos riscos;

Para a realização da análise dos riscos, optou por avaliar a probabilidade dos impactos de produtividade e requisitos legais, uma vez que desconhecia os critérios dos restantes. A classificação dos riscos foi realizada tendo por base a seguinte matriz:

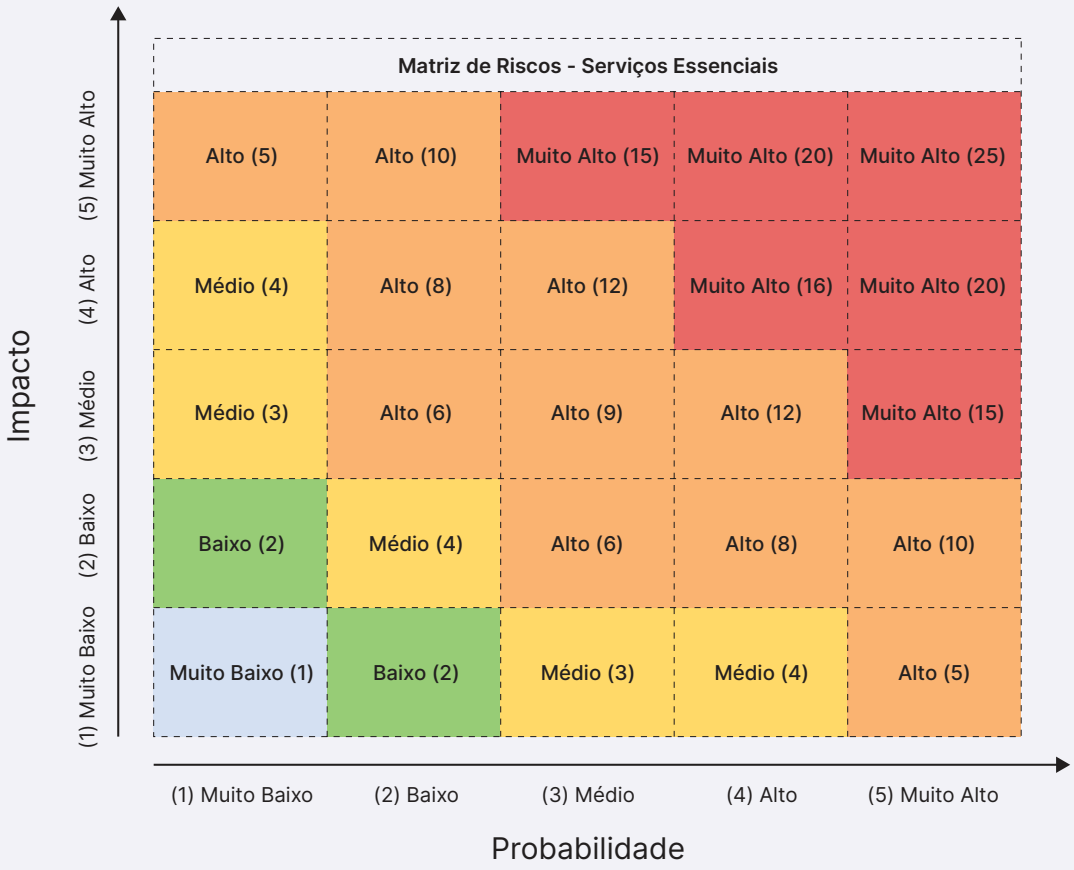

Figura 16 - Exemplo da Matriz de Risco

Tabela 15 - Exemplo da Fase de Análise dos Riscos

FASE DE ANÁLISE DOS RISCOS - EXEMPLO						
Descrição	**Impacto Produtividade**	**Impacto Requisitos Legais**	**#Imp**	**Probabilidade**	**#Prob**	**Classificação do Risco**
Indisponibilidade da plataforma devido a um ataque do tipo DDoS Distributed Denial of Service	Muito Alto	Baixo	Médio	Improvável tendo em conta	Baixo	Média
Mau funcionamento da plataforma devido a especificações pouco claras ou incompletas.	Alto	Médio	Médio	Muito improvável tendo em conta os controlos aplicados.	Muito Baixo	Baixo
Indisponibilidade da plataforma devido a falhas no processo de gestão de vulnerabilidades	Alto	Médio	Médio	Provável tendo em conta a ausência de controlos.	Alto	Alto

Etapa 3 - Avaliação dos riscos;

Face aos níveis identificados, a organização deve realizar uma priorização dos riscos, de acordo com o definido no estabelecimento do contexto, ficando priorizados da seguinte forma:

Tabela 16 - Exemplo da Avaliação dos Riscos

AVALIAÇÃO DOS RISCOS - EXEMPLO		
Descrição	**Classificação do Risco**	**Priorização**
Indisponibilidade da plataforma devido a um ataque do tipo DDoS *Distributed Denial of Service*	Médio	2º
Mau funcionamento da plataforma devido a especificações pouco claras ou incompletas.	Baixo	3º
Indisponibilidade da plataforma devido a falhas no processo de gestão de vulnerabilidades.	Alto	1º

Tendo a definição da opção de tratamento adequada, procedendo à identificação dos controlos que podem ser implementados para mitigar, evitar ou transferir o risco, bem como definir um plano de tratamento do mesmo. A organização definiu as diversas opções de tratamento que teria de implementar para os riscos identificados, justificando as opões selecionadas.

Tabela 17 - Exemplo do Tratamento dos Riscos

TRATAMENTO DOS RISCOS - EXEMPLO			
Descrição	**Classificação do Risco**	**Opção de Tratamento**	**Justificação**
Indisponibilidade da plataforma devido a um ataque do tipo DDoS *Distributed Denial of Service*	Médio	TRANSFERIR	O prestador de serviços gere toda a infraestrutura e garante capacidades adicionais de monitorização de segurança.
Mau funcionamento da plataforma devido a especificações pouco claras ou incompletas.	Baixo	ACEITAR	Controlos aplicados em conformidade com as boas práticas nacionais e internacionais.
Indisponibilidade da plataforma devido a falhas no processo de gestão de vulnerabilidades.	Alto	MITIGAR	Incluir procedimentos de gestão e reporte de vulnerabilidades de Segurança de Informação à plataforma no contrato de prestação de serviços

X. ANEXOS

A. Catálogo de ameaças comuns

A Tabela a seguir contém exemplos de ameaças comuns. A lista pode ser usada durante o processo de avaliação dos riscos. Ameaças podem ser intencionais, acidentais ou de origem ambiental (natural).

A lista também indica, para cada tipo de ameaça, se ela pode ser considerada I (intencional), A (acidental) ou N (natural).

Tabela 18 - Exemplos de ameaças comuns

Tipos de Ameaças	Exemplos de Ameaças Comuns	Origem
i) Falha de sistema	Falha de equipamento ou sistema	A
	Saturação do sistema de informação	A, I
	Violação das condições de uso do sistema de informação que possibilitam a sua manutenção	A, I
	Defeitos (“bugs”) no sistema	A, I
	Abuso de direitos ou permissões	A, I
ii) Fenómeno natural	Fenómeno climático	N
	Fenómeno sísmico	N
	Fenómeno vulcânico	N
	Fenómeno meteorológico	N
	Inundação	N
	Fenómeno pandémico/epidémico	N
iii) Erro humano	Divulgação indevida de informação	A, I
	Introdução de dados de fontes não confiáveis	A, I
	Utilização indevida de equipamentos	A, I
	Erro na utilização	A
	Acesso não autorizado a sistemas	A, I
	Uso de cópias de software falsificadas ou ilegais	A, N, I
	Adulteração de software	A, I
	Violação de leis e regulamentos	A, I

Tipos de Ameaças	Exemplos de Ameaças Comuns	Origem
iv) Ataque malicioso	Terrorismo, sabotagem	I
	Engenharia social	I
	Interceção de informações	I
	Ciberespionagem, escuta não autorizada	I
	Furto de dispositivos de armazenamento, documentos ou informação	I
	Furto de credenciais ou identidade digital	I
	Furto de equipamentos	I
	Recuperação de dispositivos de armazenamento reciclados ou descartados	I
	Divulgação de informações	A, I
	Introdução de dados de fontes não confiáveis	A, I
	Adulteração do hardware	I
	Adulteração do software	A, I
	Adulteração/Comprometimento de dados	A, I
	Exploração usando comunicações web	I
	Tratamento não autorizado de dados pessoais	I
	Entrada não autorizada nas instalações	I
	Utilização não autorizada de equipamento ou dispositivo	I
	Dano de equipamentos ou dispositivos	A, I
	Envio ou distribuição de malware	A, I
	Intrusão em sistemas ou acesso não autorizado	I
	Spoofing (fazer-se passar por outro);	I
	Ataque a sistemas (por exemplo, ataque distribuído de negação de serviço);	I
	Chantagem, suborno, agressão ou extorsão a funcionários	I
	Uso impróprio de recurso computacional	I
	Forjamento de direitos	I
v) Falha no fornecimento de bens ou serviços por terceiro	Interrupção no sistema de abastecimento	A, I
	Interrupção no sistema de refrigeração ou ventilação	A, I
	Perda do fornecimento de energia	A, N, I
	Interrupção do fornecimento do serviço de telecomunicações	A, I
	Interrupção de equipamento de telecomunicações	A, I
v) Outros;	Fogo	A, N, I
	Água	A, N, I
	Poluição, radiação nociva	A, N, I
	Acidente grave	A, N, I
	Explosão	A, N, I
	Poeira, corrosão, congelamento	A, N, I
	Radiação eletromagnética	A, N, I
	Radiação térmica	A, N, I
	Impulsos eletromagnéticos	A, N, I
	Falta de recursos humanos	A, N
	Falta de recursos	A, N

B. Catálogo de vulnerabilidades

A Tabela a seguir contém alguns exemplos de vulnerabilidades. A lista pode ser usada durante o processo de avaliação dos riscos.

Tabela 19 - Catálogos de vulnerabilidades

Tipos	Exemplos de vulnerabilidades
Hardware	Manutenção insuficiente/Instalação defeituosa de dispositivos de armazenamento
	Falta de uma rotina de substituição periódica
	Suscetibilidade à humidade, poeira, sujeira
	Sensibilidade à radiação eletromagnética
	Inexistência de um controlo eficiente de mudança de configuração
	Suscetibilidade a variações de voltagem
	Suscetibilidade a variações de temperatura
	Armazenamento não protegido
	Falta de cuidado durante o descarte ou destruição
	Realização não controlada de cópias
Software	Procedimentos de teste de software insuficientes ou inexistentes
	Falhas conhecidas no software
	Não execução do término de sessão (logout) ao deixar-se uma estação de trabalho sem assistência / controlo
	Destruição ou reutilização de dispositivos de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados
	Inexistência de um registo de auditoria
	Atribuição indevida de direitos de acesso
	Software amplamente distribuído
	Utilizar programas com um conjunto errado de dados (referentes a um outro período)
	Interface de utilizador complexa
	Documentação inexistente ou insuficiente
	Configuração incorreta de parâmetros
	Datas incorretas
	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
	Listas de passwords desprotegidas
	Fraca gestão de passwords
	Serviços desnecessários permanecem habilitados
	Software novo ou imaturo
	Especificações confusas ou incompletas para os programadores
	Inexistência de um controlo eficaz de mudança
	Download e uso não controlado de software
	Falta ou inexistência de cópias de segurança (“backup”)
	Inexistência de relatórios de gestão

Tipos	Exemplos de vulnerabilidades
Rede	Inexistência ou insuficientes evidências que comprovem o envio ou receção de mensagens
	Linhas de comunicação desprotegidas
	Tráfego sensível desprotegido
	Junções de cablagem mal feitas
	Ponto único de falha
	Falta ou ineficácia de mecanismos de identificação e autenticação do emissor e do recetor
	Arquitetura insegura da rede
	Transferência de passwords em claro
	Gestão de rede inadequada (quanto à flexibilidade de roteamento)
	Conexões de redes públicas desprotegidas
Pessoas	Ausência de recursos humanos
	Procedimentos de recrutamento inadequados
	Formação insuficiente em segurança
	Uso incorreto de software e hardware
	Falta de consciencialização em segurança
	Inexistência ou insuficiência de mecanismos de monitorização
	Trabalho não supervisionado de pessoal de limpeza ou de terceiros
	Inexistência ou insuficiência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e salas
	Localização em área suscetível a inundações
	Fornecimento instável de energia
	Insuficientes mecanismos de proteção física no prédio, portas e janelas

Tipos	Exemplos de vulnerabilidades
Organização	Inexistência ou ineficácia na sua implementação de um procedimento formal para o registo e a remoção de utilizadores
	Inexistência ou ineficácia na sua implementação de processo formal para a análise crítica dos direitos de acesso (supervisão)
	Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros
	Inexistência ou ineficácia na sua implementação de procedimento de monitorização das instalações de processamento de informações
	Inexistência de auditorias periódicas (supervisão) regulares
	Inexistência ou ineficácia na sua implementação de procedimentos para a identificação, análise e avaliação dos riscos
	Inexistência ou insuficientes relatórios de falha nos arquivos (“logs”) de auditoria das atividades de administradores e operadores
	Resposta inadequada do serviço de manutenção
	Service Level Agreement (SLA) inexistente ou insuficiente
	Inexistência ou ineficácia na sua implementação de procedimento de controlo de mudanças
	Inexistência ou ineficácia na sua implementação de um procedimento formal para o controlo da documentação do SGSI – Sistema de Gestão de Segurança da Informação
	Inexistência ou ineficácia na sua implementação de um procedimento formal para a supervisão dos registos do SGSI
	Inexistência ou ineficácia na sua implementação de um processo formal para a autorização de informações passiveis de disponibilização publica
	Atribuição inadequada das responsabilidades de segurança da informação
	Inexistência, insuficiência ou desatualização de um plano de continuidade
	Inexistência ou ineficácia na sua implementação de política de uso de e-mail
	Inexistência ou ineficácia na sua implementação de procedimentos para a instalação de software em sistemas operativos
	Inexistência ou ineficácia na sua implementação de procedimentos para o manuseamento de informações classificadas
	Ausência das responsabilidades ligadas à segurança da informação nas descrições de cargos e funções
	Insuficiência ou inexistência de cláusulas (relativas à segurança da informação) em contratos com funcionários
	Inexistência ou inadequação de um processo disciplinar no caso de incidentes relacionados com a segurança da informação
	Inexistência ou inadequação de uma política formal sobre o uso de dispositivos móveis
	Insuficiente controlo de ativos fora das instalações
	Política de mesas e ecrãs limpos (“clear desk and clear screen”) inexistente ou insuficiente
	Inexistência de, ou falha na autorização para as instalações de processamento de informações.
	Inexistência ou insuficiência dos mecanismos de monitorização de violações da segurança
	Inexistência ou ineficácia na implementação de procedimentos para o reporte de fragilidades ligadas à segurança.
	Inexistência ou ineficácia na implementação de procedimentos para garantir a conformidade com os direitos de propriedade intelectual

GOVEIN 19

Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia