CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

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

Centro Nacional de Cibersegurança

V 1.0

Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

ÍNDICE

I. SUMÁRIO EXECUTIVO 4

II. INTRODUÇÃO 5

A. ENQUADRAMENTO 5

B. CONTEXTO LEGISLATIVO E REFERENCIAL 6

C. PÚBLICO-ALVO 9

D. DEFINIÇÕES E ABREVIATURAS 9

a) DEFINIÇÕES 9

b) ABREVIATURAS 11

E. ESTRUTURA DO DOCUMENTO 11

III. GESTÃO DE RISCO 13

A. CONSIDERAÇÕES INICIAIS 13

B. ESTABELECER O CONTEXTO 16

a) MATRIZ RACI 19

IV. PROCESSO DE LEVANTAMENTO DE RISCOS 20

ETAPA 1 - IDENTIFICAÇÃO DOS RISCOS 21

a) IDENTIFICAÇÃO E VALORIZAÇÃO DE ATIVOS 23

b) IDENTIFICAÇAO DAS AMEAÇAS 25

c) IDENTIFICAÇÃO DOS CONTROLOS EXISTENTES 27

d) IDENTIFICAÇÃO DAS VULNERABILIDADES 27

ETAPA 2 - ANÁLISE DE RISCOS 29

a) METODOLOGIA DE ANÁLISE DO RISCO 31

b) CRITÉRIOS DE PROBABILIDADE E IMPACTO 32

c) DETERMINAÇÃO DO NÍVEL DE RISCO 35

i. DEFINIÇÃO DO NÍVEL DE RISCO PARA SERVIÇOS ESSENCIAIS 37

ETAPA 3 - AVALIAÇÃO DOS RISCOS 38

a) IDENTIFICAÇÃO DE MATURIDADE DE CONTROLOS EXISTENTES 39

b) AVALIAÇÃO DAS CONSEQUÊNCIAS NO NEGÓCIO 40

c) LIMITES DE ACEITAÇÃO DO RISCO 41

d) PRIORIZAÇÃO DE ACORDO COM O NÍVEL DE RISCO E A RELEVÂNCIA PARA O NEGÓCIO 41

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

V. TRATAMENTO DO RISCO 42
VI. COMUNICAÇÃO E CONSULTA DO RISCO 47
VII. MONITORIZAÇÃO E REVISÃO DOS RISCOS 49
VIII.EXEMPLO 51
IX. ANEXOS 53
A. Catálogo de ameaças comuns 53
B. Catálogo de vulnerabilidades 56

Centro Nacional de Cibersegurança
Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

I. SUMÁRIO EXECUTIVO

A consciencialização, o compromisso e a implementação de medidas de cibersegurança e segurança da informação nas organizações é cada vez mais fundamental 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 a ameaças no ciberespaço, que devem ser endereçadas de forma preventiva, através de uma abordagem de gestão de riscos.

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

Em alinhamento 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, baseado em referenciais e boas práticas de referência. No entanto, não impede que as organizações adotem outras referências que possam estar mais alinhadas com os seus objetivos.

Através deste referencial que contempla uma abordagem sistematizada e coerente ao processo de análise, avaliação e tratamento periódico dos riscos e de aferição da forma como estes se relacionam no âmbito da prestação de um bem ou serviço, pretende-se que a organização caracterize a situação atual, defina objetivos e elenque um conjunto de ações que fomentem uma evolução positiva da sua situação no contexto da cibersegurança. 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, levando a cabo, ao longo do tempo a melhoria pretendidas na gestão dos riscos.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

II. INTRODUÇÃO

A. ENQUADRAMENTO

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

Esta metodologia de gestão dos riscos pretende servir de base orientadora aos requisitos expressos no âmbito da aplicação da Lei n. º46/2018 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.º65/2021, de 30 de julho.

Todas as entidades abrangidas devem, de acordo com o artigo 10.º do Decreto-Lei n.º 65/2021, 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.

Também relevante para este contexto de gestão dos riscos de segurança da informação e cibersegurança é o exposto no Quadro Nacional de Referência para a Cibersegurança, doravante denominado QNRCS, que pretende ser um referencial à disposição da sociedade para apoio a essa resposta sistemática.

Este Guia para Gestão de Riscos em matérias de segurança da informação e cibersegurança pretende, assim, constituir um **Referencial** e orientar as diversas entidades nacionais para a realização de um processo de gestão de riscos ao nível organizacional, tendo em conta os objetivos específicos que permitam garantir a manutenção da confidencialidade, integridade e disponibilidade da informação crítica e essencial. Através das diretrizes já estabelecidas no QNRCS 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.**

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

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*" [1].

Sendo uma característica intrínseca do risco o facto de este não poder ser totalmente eliminado, torna-se fundamental a definição e operacionalização de uma estratégia global da organização para garantir a implementação de um processo eficaz e sistematizado de gestão dos riscos, numa lógica de melhoria contínua. Este é um processo permanente e contínuo de identificação, quantificação, diagnóstico e resposta, sendo que, para que seja possível gerir o risco, as organizações devem **identificar possíveis ameaças que se possam explorar as vulnerabilidades dos ativos**, bem como quais os **níveis do risco associados**, avaliando-se a **probabilidade de ocorrência e possíveis impactos**.

O resultado destas avaliações deve permitir à organização caracterizar a situação atual, definir objetivos de segurança e elencar um conjunto de ações que fomentem uma evolução positiva da sua situação no contexto da cibersegurança e segurança da informação.

B. CONTEXTO LEGISLATIVO E REFERENCIAL

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. Esta visa realizar um reforço de competências de autoridades de cibersegurança a nível nacional, aumentar a coordenação entre os Estados-Membros e assegurar a continuidade dos serviços que permitem o bom funcionamento da economia e da sociedade e que dependem fortemente das tecnologias de informação e de comunicação na União. 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

[1] Lei nº 46/2018, de 13 de agosto, que define o Regime Jurídico da Segurança do Ciberespaço

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Esta Lei aplica-se a entidades da administração pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais, bem como quaisquer outras entidades que utilizem redes e sistemas de informação, nomeadamente no âmbito da notificação voluntária de incidentes.

Com a publicação do **Decreto-Lei n.º 65/2021 de 30 de julho** procede-se à regulamentação dos aspetos remetidos para legislação complementar na Lei n.º 46/2018, de 13 de agosto. Neste sentido, o Decreto-Lei estabelece os requisitos de segurança das redes e sistemas de informação e de notificação de incidentes que devem ser cumpridos pelas entidades identificadas na Diretiva SRI – entidades da Administração Pública, Operadores de Infraestruturas Críticas, Operadores de Serviços Essenciais dos setores da energia, transportes, bancário, infraestruturas do mercado financeiro, saúde, fornecimento e distribuição de água potável e infraestruturas digitais e pelos prestadores de serviços digitais. 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 entanto, não enquadrado no presente Guia.

De acordo com o **Artigo 10.º do Decreto-Lei n.º 65/2021 de 30 de julho**, 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. 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.

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.

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

Para o 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[2] e NP ISO/IEC 31000[3].

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, nas suas diversas componentes, envolvendo toda a sua estrutura e tendo em consideração os aspetos humanos, tecnológicos e processuais. Este documento apresenta um conjunto de recomendações com vista implementação de medidas de Identificação, Proteção, Deteção, Resposta e Recuperação contra ameaças que colocam em causa a segurança do ciberespaço.

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[4]. 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. Em geral, a metodologia de gestão dos riscos ISO/IEC 27005, por ser direcionada a sistemas de informação, pode ser aplicável a todos os tipos de organização.

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

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

C. PÚBLICO-ALVO

Este Guia para Gestão de 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 parte de 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	Qualquer coisa que tenha valor para uma organização	ISO/IEC 22000
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
Consequência	Resultado de um evento que afeta os objetivos	ISO 73:2009
Controlos	Conjunto de medidas que permite modificar o risco	ISO/IEC 27000:2018

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

Evento	Ocorrência ou alteração de um conjunto particular de circunstâncias	ISO 73:2009
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
Incidente de Segurança	Qualquer evento que não faça parte do comportamento padrão de segurança, causando assim um impacto real, seja na redução ou perda total de confidencialidade, integridade ou disponibilidade de dados e informação	ISO/IEC 27000:2018
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
Vulnerabilidade	Fraqueza de um ativo ou controlo que pode ser explorada por uma ou mais ameaças.	ISO/IEC 27000:2018
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[5]
Sistema de Gestão de 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 27000:2018

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

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

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 de 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 das terminologias utilizadas.

No capítulo "**GESTÃO DE RISCO**" apresenta-se a primeira fase do processo de gestão de 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 DE 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 de riscos decompõe-se nas seguintes atividades:

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

- 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 final do documento, é apresentado um **Exemplo** através da aplicação prática da metodologia descrita neste Guia para Gestão de Riscos em Matérias de Segurança da Informação e Cibersegurança, assim como os respetivos **Anexos** ao documento.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

III. GESTÃO DE RISCO

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 na prestação do bem ou serviço.

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 da incerteza e determinação das ações necessárias, para que esta possa ser minimizada para níveis considerados aceitáveis por parte da organização.

Neste sentido, importa introduzir 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.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

O processo de gestão de riscos é um exercício estruturado, no âmbito do 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.

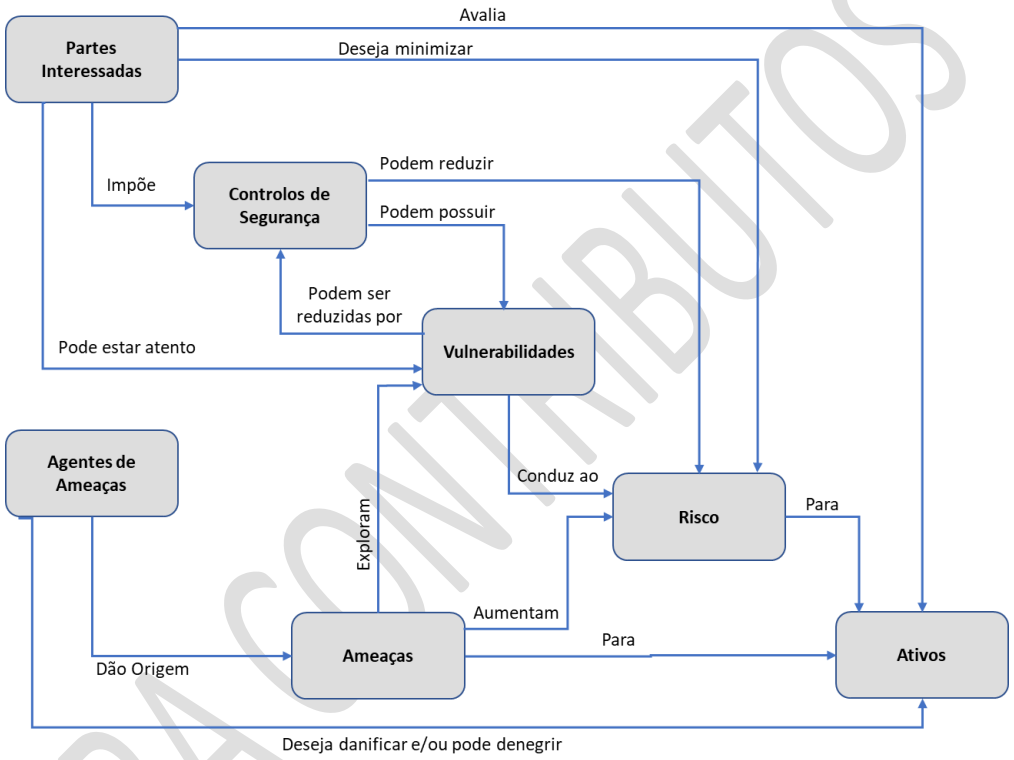

Figura 1 – Conceitos de segurança e as suas relações - adaptação da Norma ISO/ IEC 15408-1

A **Figura 2** apresenta o processo de gestão de risco baseada na norma ISO/IEC 27005, sendo composta pelas seguintes fases:

- Estabelecer Contexto;
- Levantamento de Risco (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.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

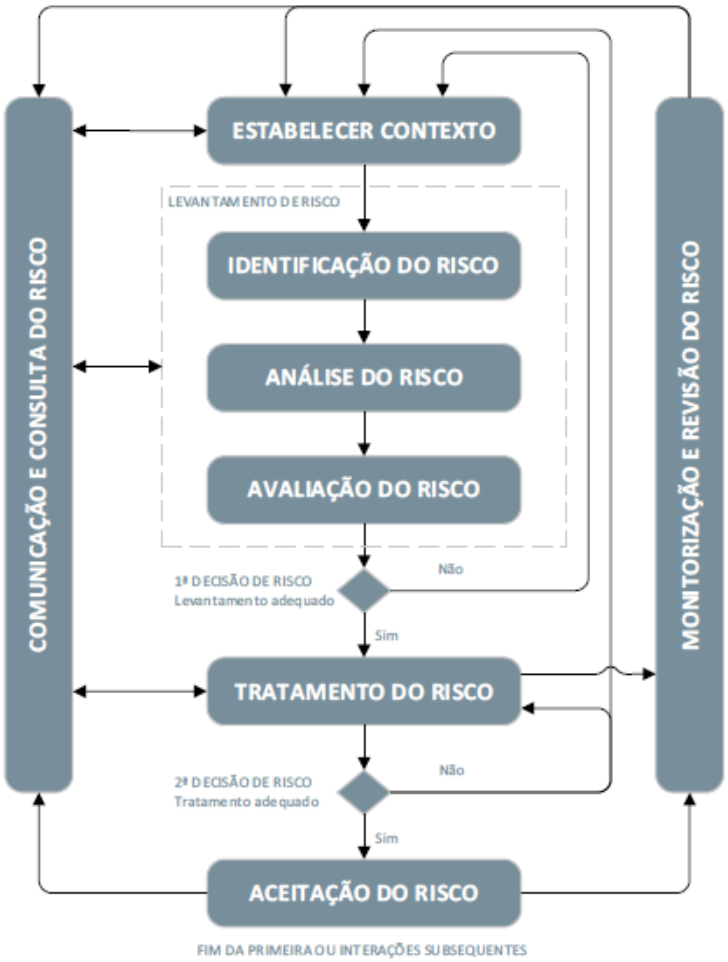

Figura 2 - Processo de Gestão de Risco; Fonte: ISO/IEC 27005:2018

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

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

B. ESTABELECER O CONTEXTO

A fase de **Estabelecer o Contexto** (**Figura 3**) no processo de gestão de riscos é essencial para o planeamento e implementação do mesmo, uma vez que permite compreender os critérios, decisões, recursos e matérias internas e externas relevantes ao propósito da organização, e que possam afetar a sua capacidade de alcançar os objetivos definidos.

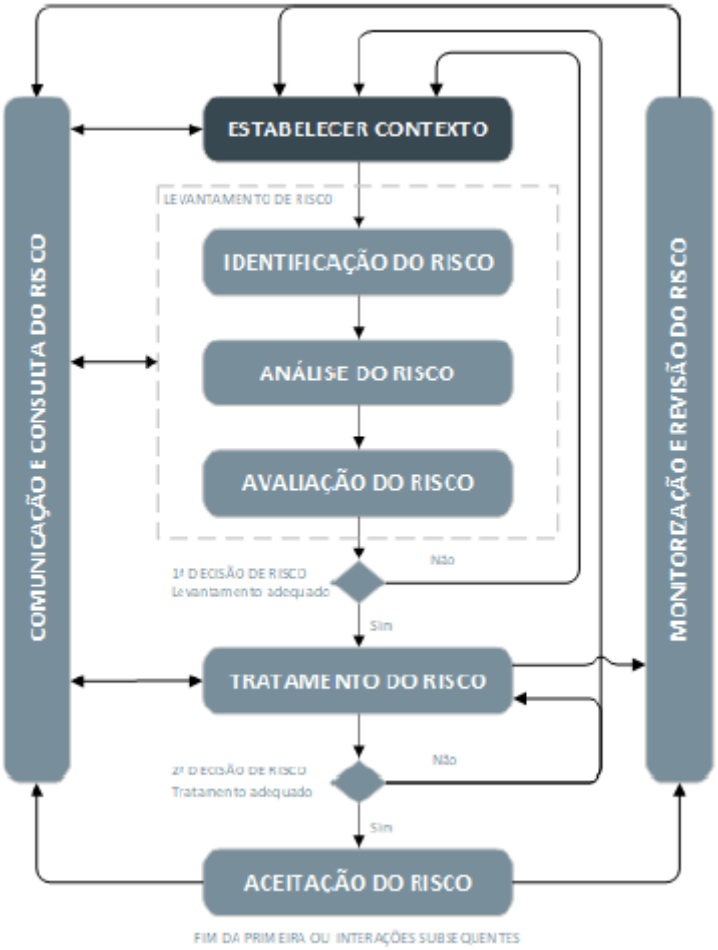

Figura 3 - "Estabelecer Contexto"- Processo de Gestão de Risco; Fonte: ISO/IEC 27005:2018

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

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

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 de risco.
Gestor de Risco	Responsável intermédio que gere o risco na organização de forma transversal	• Controlar processo de gestão dos riscos da organização; • Assegurar que a recolha de toda a informação necessária para a identificação do risco é realizada; • Assegurar que toda a informação necessária para a análise é recolhida; • Assegurar a realização da análise dos riscos; • Assegurar que as opções escolhidas para tratar os riscos são as mais corretas; • 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 a *framework* interna da gestão de risco é comunicada 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 de risco	• Gerir ativos ou sistemas de informação e os seus respetivos riscos e participar no processo de gestão dos riscos. • Assegurar que o risco é reportado ao Gestor do Risco; • Assegurar que o risco é identificado, analisado, avaliado e tratado; • Assegurar que as opções de tratamento são cumpridas.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

Note-se que identificando o modelo de governação mais adequado para a realidade organizacional, é necessário também definir processo de escalonamento associado.

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 processos para o tratamento do risco.

Outra atividade de real importância nesta fase inicial é a definição do âmbito e fronteiras do processo de gestão de riscos que irá ocorrer, definindo e delimitando todos os pontos fronteira, e que deverão ser devidamente fundamentados.

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*)**
• Ferramentas e técnicas de aferição de risco • Necessidades e expectativas das partes interessadas • Visão e obrigações da organização • Visões das partes interessadas • Objetivos da organização em matérias de requisitos de segurança da informação e cibersegurança	• Definição do âmbito e fronteiras da 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 • Definição dos papéis e responsabilidades, internos e externos	• Âmbito e fronteiras documentadas • Abordagem ao risco definida. • Matriz RACI do processo de gestão de 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 de riscos será aplicado, assim como os recursos necessários para a operacionalização do mesmo. É importante ressalvar que todas as decisões

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

tomadas no decorrer desta etapa devem ser 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**	**Gestão do Risco**	**Dono do Risco**
Atividade A	I	R, A	R, C
Atividade B	I	C	R
Atividade C	R	C	I

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

IV. PROCESSO DE LEVANTAMENTO DE RISCOS

O processo de **Levantamento de Riscos** quantifica e descreve o risco qualitativamente e capacita as organizações a priorizar os riscos de acordo com a sua gravidade percebida ou com outros critérios estabelecidos.

O processo de levantamento de riscos consiste nas seguintes atividades:

- Identificação do risco (etapa 1);
- Análise do risco (etapa 2);
- Avaliação do risco (etapa 3).

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

A etapa de avaliação de riscos é executada frequentemente em duas (ou mais) iterações. Inicialmente, uma avaliação de alto nível é realizada 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 de riscos.

O propósito da 'Identificação dos Riscos' (**Figura 4**) é determinar as ocorrências que poderão causar uma potencial perda à organização e deixar claro como, onde e porquê esta perda pode acontecer.

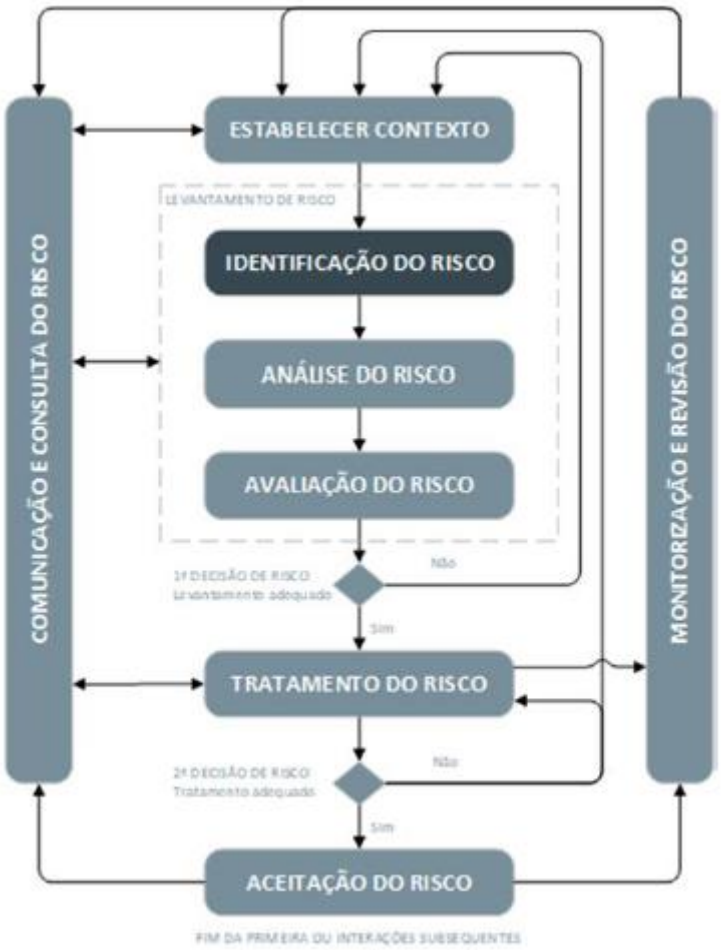

Figura 4 - "Identificação do Risco" - Processo de Gestão de Risco; Fonte: ISO/IEC 27005:2018

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 tenham sido listadas e todos os riscos delas decorrentes tenham sido identificados.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

As informações importantes para a identificação de riscos devem ser pertinentes e atualizadas, garantindo-se o envolvimento de recursos com o adequado conhecimento, e que são aplicadas técnicas de identificação de 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 avaliados;
- Questionários com gestores ou responsáveis pelos processos avaliados;
- Análise de cenários de ameaça internas e externas;
- Oficinas de avaliação de riscos (*workshops*);
- Investigação de incidentes de cibersegurança;
- Auditorias de segurança;
- Comunicação com fornecedores, parceiros e clientes;
- *Assessments* de 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, 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; • Taxonomias e outras fontes externas.	• Identificação 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 de riscos.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

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

As atividades descritas na **Tabela 6** auxiliam na recolha dos dados de entrada para a atividade de **Análise dos Riscos** (descrita no próximo subcapítulo).

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" [6] 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 10º do Decreto-Lei nº65/2021 de 30 de julho deve ser realizado para os ativos identificados no inventário de ativos (artigo 6º), no entanto, para entidades que já possuem um maior grau de maturidade e que já apliquem processos de gestão de risco, devem privilegiar uma análise mais holística comtemplando também as categorias de pessoas, localização, informação etc.

[6] Regulamento n. º183/2022 que configura instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

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

A identificação ou inventariação de ativos não é um procedimento exclusivo do processo de gestão de risco, sendo uma atividade fundamental para a gestão e operacionalização de uma adequada estratégia de segurança da informação e cibersegurança. Seja através de uma ferramenta ou aplicação de gestão de ativos ou de um catálogo de serviços informáticos aprovado, esta base de dados deve fornece informação necessária para perceber a classificação do ativo de acordo com a sua criticidade para a organização, os processos da organização que são suportados pelos ativos 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 sob estes ativos terá na atividade da organização.

Ao efetuar o inventário dos seus ativos, as entidades devem também identificar responsáveis para cada ativo. 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. O responsável pelo ativo é frequentemente a pessoa mais adequada para determinar o valor, interdependências e a criticidade do ativo para a organização.

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

Relativamente à criticidade 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 da sua importância para a organização. Esta classificação pode ter por base requisitos legais, valor, criticidade e a sensibilidade para o manuseamento da informação contida no ativo, entre outros.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

A título de exemplo, a criticidade dos ativos pode ser determinada pelo valor de reposição do ativo, nomeadamente recuperação, limpeza ou substituição da informação. Outra forma de valorização dos ativos poderá ser em função dos valores de Confidencialidade, Integridade e Disponibilidade, aplicando-se uma média dos valores referentes a estas dimensões.

(Confidencialidade + Integridade + Disponibilidade) / 3 = Valorização de ativo

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

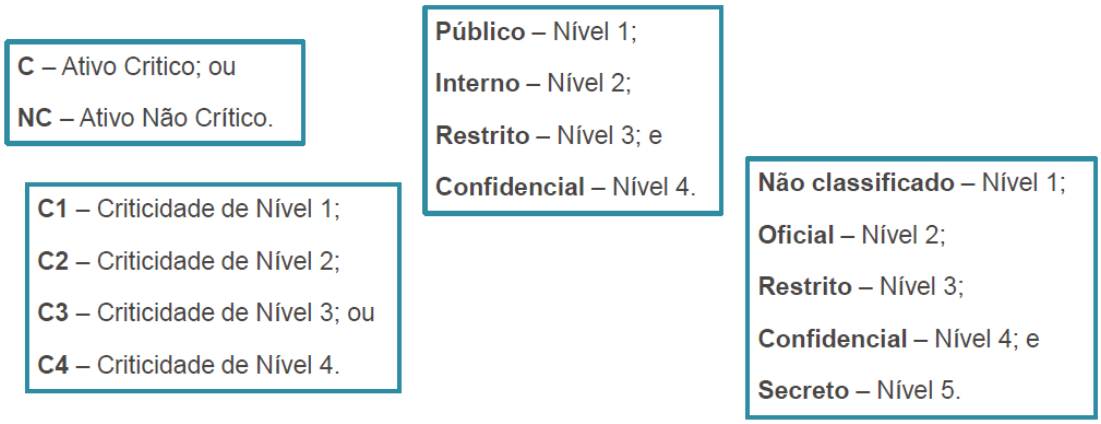

Figura 5 - Níveis de classificação dos ativos

Note-se que ao invés de realizar o processo de gestão de riscos orientados ao ativo, o mesmo poderá ser realizado a nível de "processo", tal como a ISO 9001 preconiza, fazendo-se associação a processo de negócio – ativo – risco.

b) IDENTIFICAÇAO 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, pode 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 informação sobre possíveis ameaças pode ser obtida das seguintes formas:

- Revisão de incidentes ocorridos;

- Auscultação do responsável pelo ativo;
- Perceção dos utilizadores;
- Pareceres de especialistas de segurança da informação e segurança física;
- Informações dos departamentos legais;
- Informação veiculada através de meios de comunicação;
- Informação comunicada 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 da sua área de atuação.

De acordo com artigo 10º 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.

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

A **Tabela 7** apresenta o exemplo de um processo a ser implementado na atividade de 'Identificação das ameaças'.

Tabela 7 - Identificação das ameaças

IDENTIFICAÇÃO DAS AMEAÇAS		
Entradas (*Inputs*)	**Atividades**	**Saídas (*Outputs*)**
• Informações sobre ameaças obtidas das diversas fontes consultadas	• Identificação das ameaças e respetivas fontes de informação	• Lista de ameaças.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

c) IDENTIFICAÇÃO DOS CONTROLOS EXISTENTES

Na identificação dos vetores de risco, é necessário verificar a eficácia dos controlos implementados na organização e o seu estado de implementação e de utilização, face ao cenário atual, para evitar custos e trabalhos desnecessários.

São exemplos de controlos, 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 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.

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 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 também ser identificadas nomeadamente através do

uso de ferramentas próprias, como a realização de *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 algumas vulnerabilidades catalogadas, de forma a auxiliar a sua utilização no processo de gestão dos riscos e que são categorizadas a nível de:

- *Hardware*;
- *Software*;
- Rede;
- dos recursos humanos ou pessoas;
- do ambiente físico (local ou instalações); e
- da organização e dos 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;
- 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.

Por fim, um processo de gestão de 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.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

ETAPA 2 - ANÁLISE DE RISCOS

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

A 'Análise de Riscos' (**Figura 6**) tem como objetivo verificar quais as origens dos riscos identificados, as suas consequências e impactos e qual a probabilidade de ocorrência.

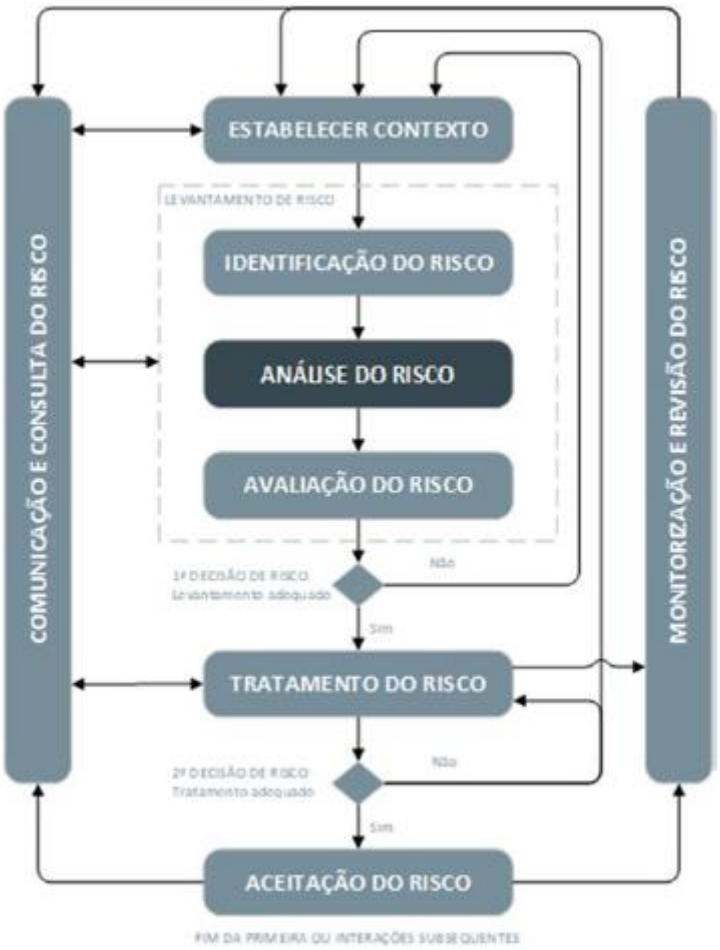

Figura 6 - "Análise do Risco" - Processo de Gestão de Risco; Fonte: ISO/IEC 27005:2018

Para execução desta fase, a organização deverá dispor de uma lista de identificação das ameaças e vulnerabilidades, dos ativos afetados e dos controlos implementados e sua eficácia, anteriormente identificados e analisados (etapa 1 de Identificação do Risco).

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

De acordo com artigo 10º do Decreto-Lei nº65/2021 de 30 de julho realização da Análise de 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.

Para uma maior compreensão dos diferentes conceitos desta etapa, considere as seguintes definições:

- **Causas:** devem ser registados os fatores de risco tanto de origem interna como externa à organização de acordo com as ameaças e as vulnerabilidades identificadas anteriormente e dentro do âmbito definido para este processo de gestão de risco;
- **Risco:** O risco é expresso como a combinação do impacto de um evento e da sua probabilidade de acontecer. Este risco é calculado sem qualquer efeito de tratamento ou de aplicação de controlos existentes.
  De forma a determinar o risco é recomendado a utilização de uma **Matriz de Riscos** (ver capítulo c) Determinação do nível de risco), registando o valor do risco como o mais alto de todas as causas identificadas.

$$\boldsymbol{Risco = Probabilidade\ x\ Impacto}$$

Essa equação pode, no entanto, ser expandida para refletir a ameaça da exploração das vulnerabilidades nos ativos, substituindo-se o conceito '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, assim sendo, pode-se reformular a equação do seguinte modo:

$$\boldsymbol{Risco = (probabilidade\ da\ ameaça\ explorar\ a\ vulnerabilidade)\ x\ (custo\ total\ do\ impacto\ do\ ativo\ explorado)}$$

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

Para qualquer uma dessas descrições de risco, a metodologia necessita atribuir valores a esses fatores. Embora existam muitas abordagens diferentes, essencialmente dividem-se em duas abordagens: qualitativos e quantitativo.

Outros conceitos importantes a considerar são:

- **Risco inerente:** O risco inerente 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) METODOLOGIA DE ANÁLISE DO RISCO

A metodologia de análise do risco 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. A análise quantitativa poderá ser desvantajosa, caso não existam dados factuais e/ou auditáveis. Esta situação pode criar uma ilusão de precisão e de eficácia do processo de avaliação do risco.

A metodologia de análise de risco a utilizar deverá ser consistente com o definido na fase de 'Estabelecer Contexto'. Neste Guia irá optar-se por uma análise do tipo qualitativa, uma vez que tem como objetivo ser aplicável a um conjunto muito diverso de organizações e facilitará a compreensão das várias partes interessadas nomeadamente no que concerne a indicadores gerais do nível do risco e para identificar os 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 da gestão de 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 ou na opinião de especialistas.

As diretrizes para os critérios de avaliação podem ser identificadas na **Figura 7**.

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.

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 6 meses.	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 em intervalos de 1 ano ou superior.	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 até 3 anos.	Evento que gera impacto sobre um pequeno grupo ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções secundárias de trabalho, não sendo o 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 5 anos.	Evento que gera impacto sobre apenas uma pessoa ou representa perda de disponibilidade, confidencialidade e/ou integridade que não necessita de intervenção ou paralisação imediata.

Figura 7 - Critérios de análise de risco

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

A fim de realizar uma melhor aferição do impacto do risco, a organização poderá identificar um impacto global sem especificar critérios ou basear-se em potenciais consequências segundo vetores de impacto como categorizados a nível:

- **Legal ou regulatório** – qualquer consequência que a organização possa sofrer a nível legal e 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, e a perda financeira inevitável por forma a 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 de riscos a nível de saúde e segurança pessoal que deve ser garantida a colaboradores e partes interessadas da organização.

A Error! Reference source not found.**Error! Reference source not found.** apresenta uma definição de cada nível de impacto para todas as áreas de avaliação aquando da materialização de riscos, não invalidando que se possa apenas utilizar um critério de impacto genérico.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

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

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

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	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.

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

Relacionando o potencial impacto dos riscos ao negócio e a probabilidade de materialização desses 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 **Matriz de Riscos** na **Figura 8** distribui os riscos da seguinte maneira:

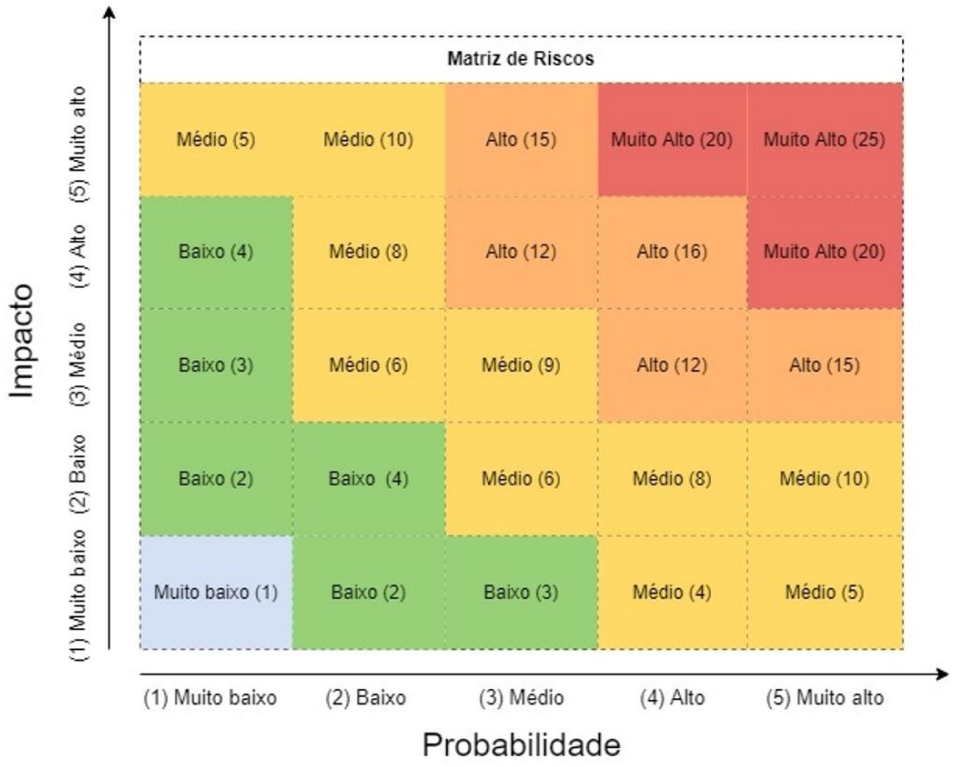

Figura 8 - Matriz de riscos

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).

Numa análise de riscos também este tipo de eventos deve ser considerado.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

i. 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 nos setores e subsetores constantes no anexo ao RJSC.

Atendendo à própria definição de OES, acredita-se que uma falha ou interrupção de um serviço essencial terá um impacto mais relevante ou substancial 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.

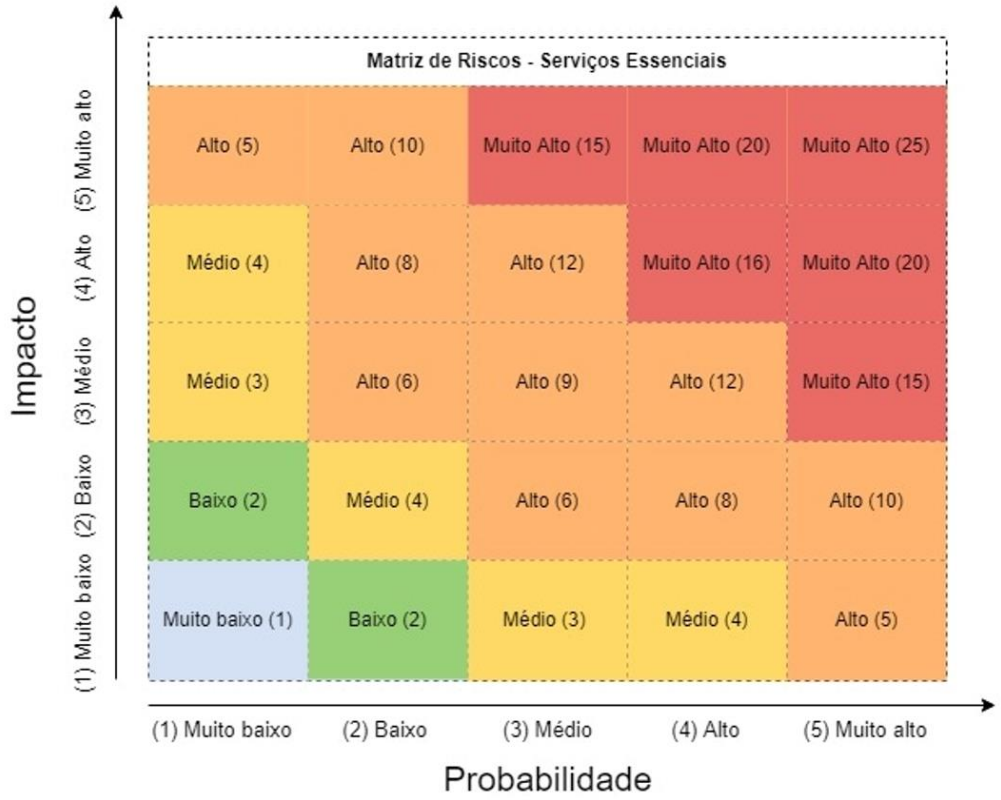

Figura 9 - Matriz de risco para os operadores de serviços essenciais

Nesta etapa da na análise do risco, é assignado a cada cenário identificado um valor ao impacto e probabilidade.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

ETAPA 3 - AVALIAÇÃO DOS RISCOS

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

A 'Avaliação dos Riscos' (**Figura 10**) 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 análise e definição do nível dos riscos inerentes 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.

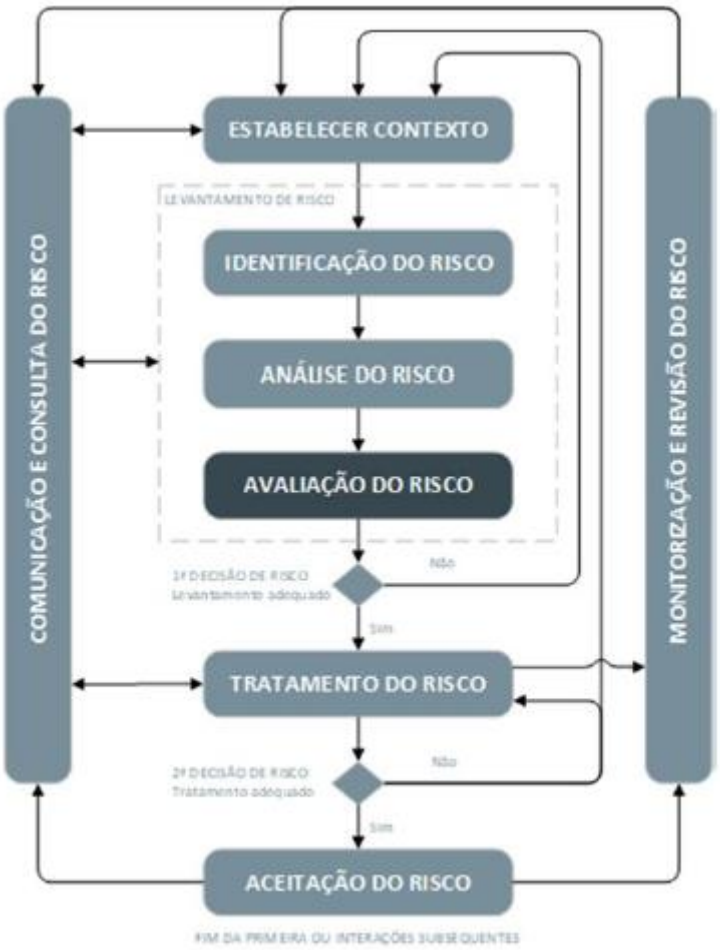

Figura 10 - "Avaliação do Risco" - Processo de Gestão de Risco; Fonte: ISO/IEC 27005:2018

Esta fase da avaliação de riscos permite uma deliberação consciente sobre quais os tratamentos que devem ser usados e por que ordem 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 de riscos de segurança da informação e cibersegurança são:

a) IDENTIFICAÇÃO DE MATURIDADE DE CONTROLOS EXISTENTES

Até este passo já é conhecido o risco inerente, pelo que realizando uma análise dos controlos que mitigam o risco inerente, passa-se a conhecer o risco real.

Ao identificar os fatores de risco, é necessário verificar a eficácia dos controlos já implementados na organização, a fim de se evitar custos e trabalho desnecessários, como, por exemplo, na duplicação de controlos. Na identificação dos controlos existe a necessidade de realizar uma verificação dos mesmos de modo a assegurar o seu correto funcionamento, uma vez que um controlo mal implementado pode originar uma vulnerabilidade.

Os controlos são medidas que modificam o risco. 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.

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 9**, 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.**

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

Tabela 9 - 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.

b) AVALIAÇÃO DAS CONSEQUÊNCIAS NO NEGÓCIO

Neste passo já é conhecido o risco real a que o serviço está exposto, uma vez que já se reduziu o valor do risco inerente consoante o nível médio aferido de maturidade dos controlos respetivos.

Neste âmbito é onde se fará a avaliação propriamente dita dos cenários de eventos identificados como relevantes para as atividades da empresa, incluindo a identificação de ameaças, vulnerabilidades, ativos afetados e consequências para os ativos, controlos existentes e processos de negócio, visando medir o potencial impacto sobre a organização. Devem ser consideradas as consequências de violações da segurança da informação, como, por exemplo: perda de confidencialidade, integridade ou disponibilidade dos ativos.

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.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

c) 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 no caso do risco estar associado a uma atividade temporária ou de curto prazo da organização.

d) 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.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

V. TRATAMENTO DO RISCO

A fase de 'Tratamento de Riscos' **(Figura 11**) 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 análise de risco.

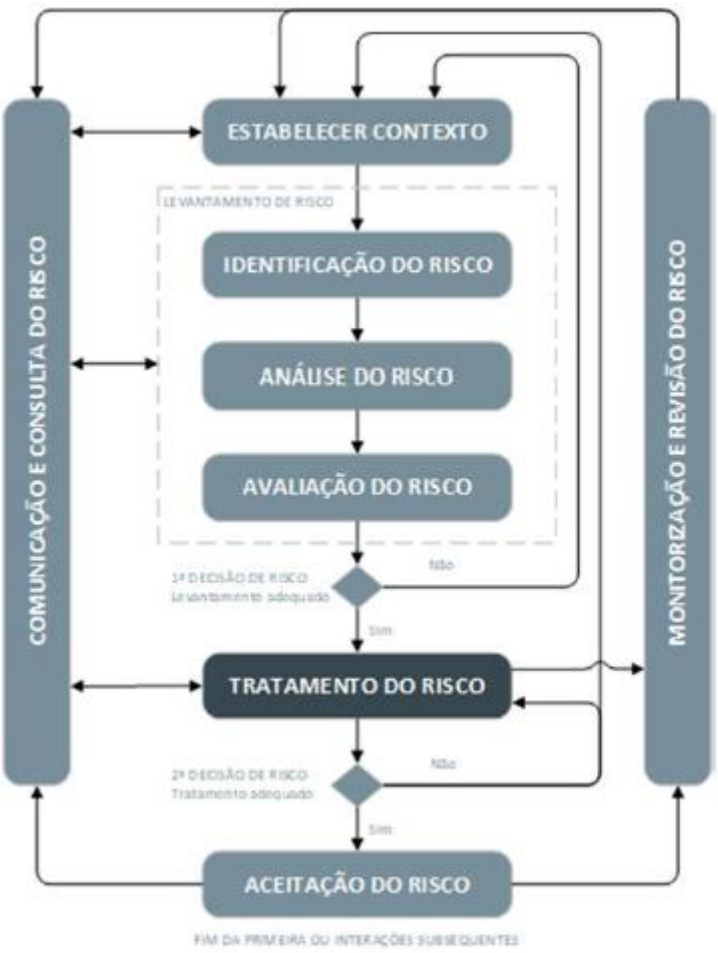

Figura 11 - "Tratamento do risco" - Processo de Gestão de Risco; Fonte: ISO/IEC 27005:2018

Para cada ação, é imprescindível que seja definido um responsável e uma data para a implementação. O objetivo é que, uma vez concluídos os planos de ação estes devem gerar novas iniciativas de mitigação ou melhoramento das já existentes, reduzindo, em consequência, o nível de risco.

Por outras palavras, o tratamento de riscos é um processo cíclico, composto por várias fases, as quais, em linhas gerais, consistem em:

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

- Avaliar o tratamento de 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.

A **Tabela 10** apresenta o exemplo de um processo a ser implementado na atividade de 'Tratamento de Riscos'.

Tabela 10 - Tratamento de risco

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

Após seguidos os passos apresentados na Tabela 10**,** o ciclo de avaliação e implementação de tratamento de riscos recomeça.

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 de risco 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. Somente riscos de nível baixo e muito baixo podem ser retidos; suportar 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. Esta opção é 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 11** apresenta um exemplo do tratamento recomendado para cada valor de risco identificado:

Tabela 11 - Exemplo de Tratamento de risco

Valor do Risco Inerente e 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 tem como responsabilidade a avaliação e elaboração dos planos de tratamento de riscos de acordo com o processo de tratamento ilustrado na **Figura 12.**

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

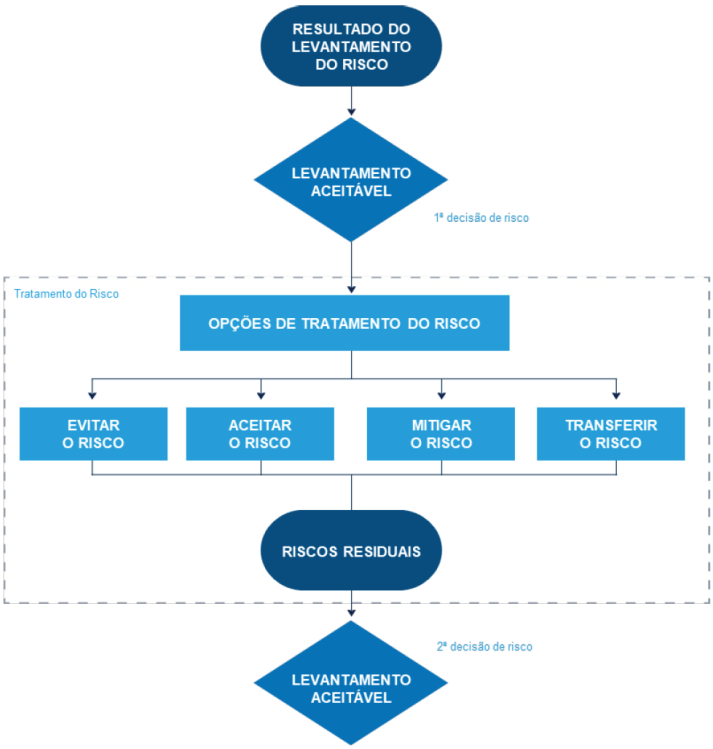

Figura 12 - Tratamento do Risco; Fonte: ISO/IEC 27005

Os riscos identificados como "Muito Altos" devem ser, obrigatoriamente, tratados. Os OSE devem, obrigatoriamente, tratar todos os riscos classificados como "Alto" e "Muito Alto".

As opções para o tratamento dos riscos são diversas e podem ser implementadas de forma individual ou simultaneamente. A seleção das opções mais adequadas para cada caso analisado 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, por outro lado, os prejuízos que tal tratamento estará evitando ou prevenindo.

Os planos de tratamento de riscos servem para documentar quais as opções de tratamento que foram selecionadas e 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.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

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

Os planos de tratamento de riscos de segurança da informação e cibersegurança devem ser endereçados na Matriz de Riscos, para o correto acompanhamento e tratamentos dos riscos identificados.

VI. COMUNICAÇÃO E CONSULTA DO RISCO

A "Comunicação do Risco" (**Figura 13**) é uma atividade que tem como objetivo alcançar 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. Esta comunicação é importante pois os tratamentos igualmente eficazes podem ser mais aceitáveis para algumas partes do que para outras, considerando-se os interesses e objetivos comuns e particulares.

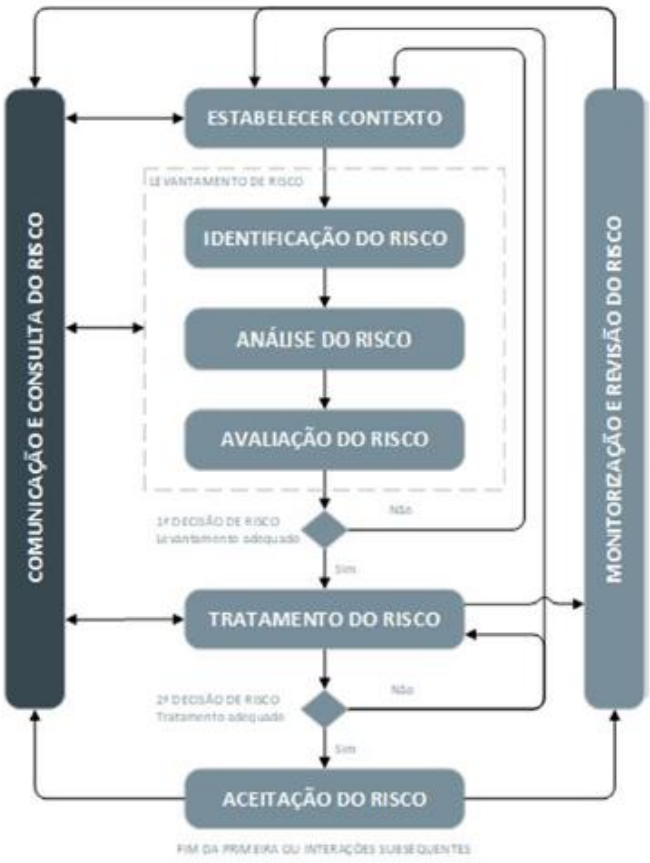

Figura 13 - "Comunicação e Consulta do Risco" -Processo de Gestão do Risco; Fonte: ISO/IEC 27005:2018

É fundamental compreender que sem a consolidação de uma cultura de gestão dos riscos na organização, os objetivos e a segurança que se pretendem atingir poderão ser comprometidos.

Assim, deve ressaltar-se a importância de implementar uma cultura de gestão dos riscos, através da divulgação regular do conhecimento gerado pela aplicação do Guia para Gestão de riscos na organização e envolvimento das diferentes partes interessadas. Também a realização periódica da revisão dos riscos e verificação do estado dos planos de tratamento de riscos de segurança

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

da informação e de cibersegurança, com apresentações e análise dos resultados à Gestão de Topo deve ser considerada.

Na **Tabela 12** é possível identificar as atividades relativas à comunicação e consulta do risco.

Tabela 12 - Comunicação e consulta

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

A organização deverá estabelecer um plano 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 de risco 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.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

VII. MONITORIZAÇÃO E REVISÃO DOS RISCOS

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.

A monitorização e a análise crítica podem ser realizadas de forma periódica, necessária à manutenção do ciclo de gestão dos riscos e à melhoria contínua do processo, como também na ocorrência de um evento específico.

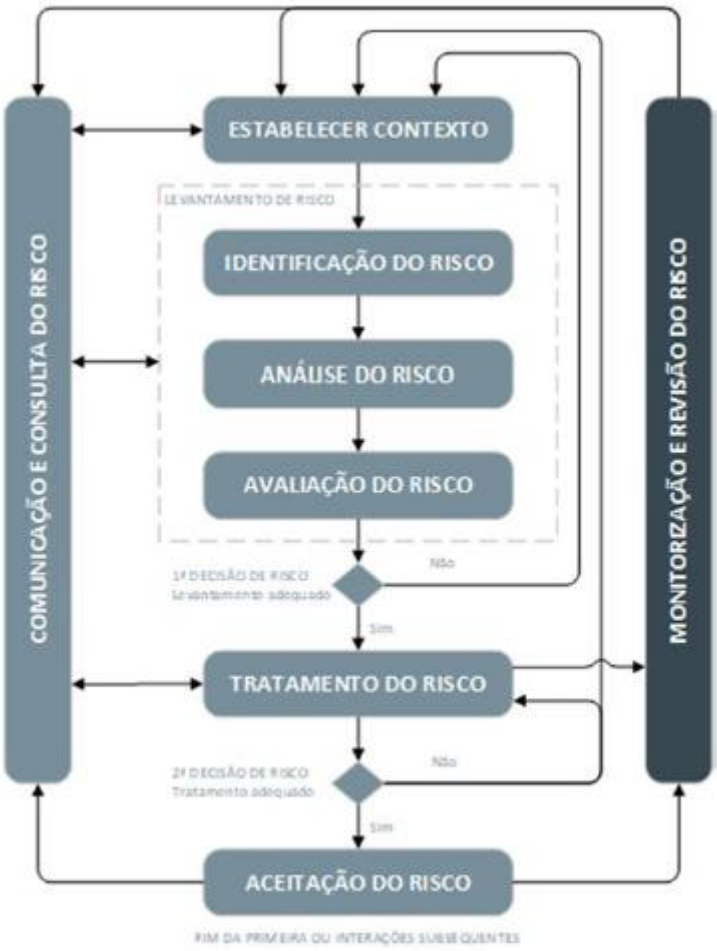

Figura 14 – "Monitorização e Revisão do Risco" - Processo de Gestão de Risco; Fonte: ISO/IEC 27005:2018

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

- verificar a eficácia e a eficiência dos controlos implementados;

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

- obter informações adicionais para melhoria do processo de avaliação de riscos como um todo;
- analisar eventos e possíveis incidentes, para que seja possível aprender com eles;
- 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 sejam registados, para que se possa estudá-los e aperfeiçoar contínua e progressivamente o processo de gestão de riscos de segurança da informação, além de auxiliar na análise de desempenho dos procedimentos, métodos e ferramentas implementados.

A organização deve garantir que os seguintes pontos são monitorizados de forma contínua:

- 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 a requisitos de negócios modificados);
- 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 possam ocorrer.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

VIII. EXEMPLO

O João, responsável do Gabinete de Gestão de Projeto da Organização, identificou a necessidade da realização da análise de risco 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 de risco e definição de âmbito e fronteiras, entre outras.

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;
- Etapa 2 - Análise de riscos;
- Etapa 3 - Avaliação de riscos;

Para a identificação dos riscos, o João decidiu realizar um *assessment* de riscos de segurança da informação e cibersegurança, onde fez a identificação de ativos, ameaças, controlos existentes e vulnerabilidades. Nesse sentido foi identificado o seguinte risco:

Elevada possibilidade de roubo das palavras-passe dos utilizadores da plataforma de gestão de ficheiros, alojada num serviço de computação em nuvem, que é utilizada pela organização para disponibilização de toda a documentação gerada no âmbito da execução dos seus projetos.

- Ativos: plataforma de gestão de ficheiros; documentação gerada no âmbito da execução dos projetos;
- Ameaças: ataque malicioso externo
- Controlos existentes: política de palavras-passe
- Vulnerabilidades: política de palavras-passe deficiente colocando em causa a confidencialidade e a integridade da informação que se encontrava alojada neste ativo.

Para realização da análise de risco, o João deve ter em conta:

- metodologia de análise de riscos: análise quantitativa do risco;
- critérios de probabilidade e impacto:
    - Impacto genérico – ‘4 – Alto’;
    - Probabilidade: ‘5 – Muito Alto’;

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

- determinação do nível de risco: ‘20 – Muito Alto’, tendo em conta a matriz de Risco definida para operadores de serviço essencial;

Face ao nível identificado, a organização não o pode aceitar, uma vez que todos os riscos de nível “Muito Alto” devem ser obrigatoriamente tratados, exceto se tiverem sido formalmente aceites pela Gestão de Topo. Nesse caso, a organização, na sua sessão de gestão do risco, pode tomar a decisão estratégica de o mitigar e de executar as seguintes atividades:

1) Garantir que o fornecedor da plataforma de gestão de ficheiros altera a sua política de gestão de palavras-passe em conformidade com as suas práticas internas, no espaço de tempo a definir;
2) Avaliar outras plataformas que prestem o mesmo serviço, com as condições consideradas como adequadas pela organização.

Foi igualmente identificada uma responsável (Inês – Diretora dos Sistemas de Informação) pela execução destas atividades de tratamento do risco, tendo sido igualmente acordada uma data estimada de resolução. A data foi escolhida de acordo com as prioridades atribuídas aos riscos identificados, tendo em conta o nível do risco e a criticidade dos ativos envolvidos.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

IX. 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 das ameaças. 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 13 - Exemplos de ameaças comuns

Tipos de Ameaças	Ameaças	Origem
i) Falha de sistema;	Falha do ar-condicionado	A
	Falha de equipamento	A
	Defeito de equipamento	A, I
	Saturação do sistema de informação	A
	Defeito de *software*	A
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	A, I
ii) Fenómeno natural;	Fenómeno climático	N
	Fenómeno sísmico	N
	Fenómeno vulcânico	N
	Fenómeno meteorológico	N
	Inundação	N
iii) Erro humano;	Divulgação indevida de informação	A, I
	Dados de fontes não confiáveis	A, I
	Alteração do *hardware*	I
	Alteração do *software*	A, I
	Acesso não autorizado a sistemas	A, I
	Uso de cópias de *software* falsificadas ou ilegais	A, N, I
	Processamento ilegal de dados	I
	Defeitos (“*bugs*”) no sistema	A, I

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

v) Falha no fornecimento de bens ou serviços por terceiro;	Interrupção do fornecimento de água	A, I
	Interrupção do fornecimento de energia	A, N, I
	Interrupção do fornecimento do serviço de telecomunicações	A, I
iv) Ataque malicioso;	Ciberespionagem	I
	Escuta não autorizada	I
	Furto de dispositivos de armazenamento ou documentos	I
	Furto de equipamentos	I
	Recuperação de dispositivos de armazenamento reciclados ou descartados	I
	Alteração do *hardware*	I
	Alteração do *software*	A, I
	Determinação da localização	I
	Engenharia social	I
	Intrusão em sistemas, infiltrações e entradas não autorizadas	I
	Acesso não autorizado a sistemas	I
	Crime digital (por exemplo, perseguição no mundo digital);	I
	Ato fraudulento (por exemplo, reutilização indevida de credenciais e dados transmitidos, fazer-se passar por uma outra pessoa, intercetação);	I
	Suborno por informação;	I
	Spoofing (fazer-se passar por outro);	I
	Utilização de Código malicioso (por exemplo: vírus, *ransomware*, Cavalo de Troia e etc.)	I
	Bomba/terrorismo;	I
	Guerra de informação;	I
	Ataque a sistemas (por exemplo, ataque distribuído de negação de serviço);	I

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

	Furto de informação	I
	Violação de dados pessoais	I
	Chantagem, suborno, agressão ou extorsão a funcionários	I
	Vasculhar informação de propriedade intelectual	I
	Uso impróprio de recurso computacional	I
	Entrada de dados falsificados ou corrompidos	I
	Intercetação de informações	I
	Sabotagem de sistemas	I
	Uso não autorizado de equipamento	I
	Cópia ilegal de *software*	I
	Uso de cópias de *software* falsificadas ou ilegais	A, N, I
	Comprometimento dos dados	A, I
	Processamento ilegal de dados	I
	Forjamento de direitos	I
v) Outros;	Fogo	A, N, I
	Água	A, N, I
	Poluição	A, N, I
	Acidente grave	A, N, I
	Destruição de equipamento ou dispositivos de armazenamento	A, N, I
	Poeira, corrosão, congelamento	A, N, I
	Radiação eletromagnética	A, N, I
	Radiação térmica	A, N, I
	Impulsos eletromagnéticos	A, N, I
	Erro durante o uso	A
	Abuso de direitos	A, I
	Repúdio de ações	I
	Indisponibilidade de recursos humanos	A, N, I

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

B. Catálogo de vulnerabilidades

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

Tabela 14 - Catálogos de vulnerabilidades

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Hardware	Manutenção insuficiente/Instalação defeituosa de dispositivos de armazenamento	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Falta de uma rotina de substituição periódica	Destruição de equipamento ou dispositivos de armazenamento
	Sensibilidade à humidade, poeira, sujeira	Poeira, corrosão, congelamento
	Sensibilidade à radiação eletromagnética	Radiação eletromagnética
	Inexistência de um controlo eficiente de mudança de configuração	Erro durante o uso
	Sensibilidade a variações de voltagem	Interrupção do suprimento de energia
	Sensibilidade a variações de temperatura	Fenómeno meteorológico
	Armazenamento não protegido	Furto de dispositivos de armazenamento ou documentos
	Falta de cuidado durante o descarte e a destruição	Furto de dispositivos de armazenamento ou documentos
	Realização não controlada de cópias	Furto de dispositivos de armazenamento ou documentos

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

Software	Procedimentos de teste de software insuficientes ou inexistentes	Abuso de direitos
	Falhas conhecidas no software	Abuso de direitos
	Não execução do "logout" ao deixar-se uma estação de trabalho sem assistência / controlo	Abuso de direitos
	Destruição ou reutilização de dispositivos de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados	Abuso de direitos
	Inexistência de um registo de auditoria	Abuso de direitos
	Atribuição indevida de direitos de acesso	Abuso de direitos
	Software amplamente distribuído	Comprometimento dos dados
	Utilizar programas com um conjunto errado de dados (referentes a um outro período)	Comprometimento dos dados
	Interface de utilizador complexa	Erro durante o uso
	Documentação inexistente	Erro durante o uso
	Configuração de parâmetros incorreta	Erro durante o uso
	Datas incorretas	Erro durante o uso
	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores	Utilização indevida de privilégios
	Listas de passwords desprotegidas	Utilização indevida de privilégios
	Má gestão de passwords	Utilização indevida de privilégios
	Serviços desnecessários permanecem habilitados	Processamento ilegal de dados
	Software novo ou imaturo	Defeito de software

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

	Especificações confusas ou incompletas para os developers	Defeito de software
	Inexistência de um controlo eficaz de mudança	Defeito de software
	Download e uso não controlado de software	Alteração do software
	Inexistência de cópias de segurança ("backup")	Alteração do software
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de dispositivos de armazenamento ou documentos
	Inexistência de relatórios de gestão	Uso não autorizado de equipamento
Rede	Inexistência de evidências que comprovem o envio ou receção de mensagens	Repúdio de ações
	Linhas de comunicação desprotegidas	Interseção de comunicação não autorizada
	Tráfego sensível desprotegido	Interseção de comunicação não autorizada
	Junções de cablagem mal feitas	Falha do equipamento de telecomunicação
	Ponto único de falha	Falha do equipamento de telecomunicação
	Não identificação e não autenticação do emissor e do recetor	Forjamento de direitos
	Arquitetura insegura da rede	Ciberespionagem
	Transferência de *passwords* em claro	Ciberespionagem
	Gestão de rede inadequada (quanto à flexibilidade de roteamento)	Saturação do sistema de informação

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

	Conexões de redes públicas desprotegidas	Uso não autorizado de equipamento
Pessoas	Ausência de recursos humanos	Indisponibilidade de recursos humanos
	Procedimentos de recrutamento inadequados	Destruição de equipamento ou dispositivos de armazenamento
	Formação insuficiente em segurança	Erro durante o uso
	Uso incorreto de *software* e *hardware*	Erro durante o uso
	Falta de conscienlização em segurança	Erro durante o uso
	Inexistência de mecanismos de monitorização	Processamento ilegal de dados
	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados	Furto de dispositivos de armazenamento ou documentos
	Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens	Uso não autorizado de equipamento
Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos	Destruição de equipamento ou dispositivos de armazenamento
	Localização em área suscetível a inundações	Inundação
	Fornecimento de energia instável	Interrupção do suprimento de energia

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de equipamentos
Organização	Inexistência de um procedimento formal para o registo e a remoção de utilizadores	Abuso de direitos
	Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)	Abuso de direitos
	Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros	Abuso de direitos
	Inexistência de procedimento de monitorização das instalações de processamento de informações	Abuso de direitos
	Inexistência de auditorias periódicas (supervisão)	Abuso de direitos
	Inexistência de procedimentos para a identificação, análise e avaliação de riscos	Abuso de direitos
	Inexistência de relatórios de falha nos arquivos ("*logs*") de auditoria das atividades de administradores e operadores	Abuso de direitos
	Resposta inadequada do serviço de manutenção	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Service Level Agreement inexistente ou insuficiente	Violação das condições de uso do sistema de

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

		informação que possibilitam sua manutenção
	Inexistência de procedimento de controlo de mudanças	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Inexistência de um procedimento formal para o controlo da documentação do SGSI	Comprometimento dos dados
	Inexistência de um procedimento formal para a supervisão dos registos do SGSI	Comprometimento dos dados
	Inexistência de um processo formal para a autorização das informações disponíveis publicamente	Dados de fontes não confiáveis
	Atribuição inadequada das responsabilidades pela segurança da informação	Repúdio de Ações
	Inexistência de um plano de continuidade	Falha de equipamento
	Inexistência de política de uso de correspondência eletrónica (e-mail)	Utilização abusiva
	Inexistência de procedimentos para a instalação de software em sistemas operativos	Erro durante o uso
	Ausência de registos nos arquivos de auditoria (“*logs*”) de administradores e operadores	Erro durante o uso

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

	Inexistência de procedimentos para a manipulação de informações classificadas	Erro durante o uso
	Ausência das responsabilidades ligadas à segurança da informação nas descrições de cargos e funções	Erro durante o uso
	Cláusulas (relativas à segurança) insuficientes ou inexistentes, em contratos com funcionários	Processamento ilegal de dados
	Inexistência de um processo disciplinar no caso de incidentes relacionados à segurança da informação	Furto de equipamentos
	Inexistência de uma política formal sobre o uso de dispositivos móveis	Furto de equipamentos
	Inexistência de controlo sobre ativos fora das dependências	Furto de equipamentos
	Política de mesas e ecrãs limpos ("*clear desk and clear screen*") inexistente ou insuficiente	Furto de dispositivos de armazenamento ou documentos
	Inexistência de autorização para as instalações de processamento de informações	Furto de dispositivos de armazenamento ou documentos
	Inexistência de mecanismos estabelecidos para a monitorização de violações da segurança	Furto de dispositivos de armazenamento ou documentos
	Inexistência de análises críticas periódicas por parte da direção	Uso não autorizado de equipamento

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt

	Inexistência de procedimentos para o report de fragilidades ligadas à segurança	Uso não autorizado de equipamento
	Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual	Uso de cópias de *software* falsificadas ou ilegais

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel. (+351) 21 049 74 00 | Fax (+351) 21 049 73 98 | cncs@cncs.gov.pt