
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VII – MAIO DE 2019

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW
by CIJIC

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Nesta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, antes de mais, aproveito para anunciar uma nova edição do Curso de Direito do Ciberespaço, em formato novel, a ter lugar em Novembro de 2019. À semelhança do curso anterior, na oportunidade de publicação de alguns artigos, a Revista assumir-se-á como esse veículo de partilha de conhecimento.

No que concerne propriamente às notas desta edição, permitam-me partilhar algumas novidades e preocupações.

No passado dia 23 de maio do corrente, o Conselho de Ministros aprovou a Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023, que ainda carece de publicação em jornal oficial. Não obstante é já do domínio público que o propósito desta nova ENSC visará *garantir a proteção e a defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas, procedendo desta forma à revisão da ENSC de 2015*[1], tendo em atenção a evolução digital ocorrida desde então.

1 https://www.portugal.gov.pt/pt/gc21/governo/comunicado-de-conselho-de-ministros?i=278
A propósito, neste conspecto, para quem não tenha estado presente, na Conferência – Cibersegurança, na Universidade de Évora, a 14 de novembro de 2018, será interessante dar uma vista de olhos na apresentação "A Estratégia Nacional de Segurança do Ciberespaço 2.0 – Governação e execução", feita e disponibilizada por parte do CALM Gameiro Marques, da Autoridade Nacional de Segurança, cujo conteúdo pode ser encontrado @ https://www.uevora.pt/media_informacoes/agenda/(item)/25903.

Em efeméride de aniversário do Regulamento Geral de protecção de dados, e estando este em vigor desde *o vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia*, naturalmente a «Cyberlaw by CIJIC» não poderia passar ao lado do tema, recorrente dos últimos anos.

De facto, nestes 3 anos volvidos, é inconcebível que Portugal ainda não tenha uma lei de execução do mesmo. De igual forma, é inconcebível que as organizações, públicas ou privadas, só conheçam o "consentimento" como fundamento de licitude para o tratamento de dados pessoais, considerando-o um verdadeiro *canivete-suíço*. Ainda havemos de pugnar por um "*direito ao esquecimento*" sobre o consentimento, pois que a livre revogabilidade do mesmo por parte da pessoa titular dos dados pessoais parece sucumbir ante tanto abuso na sua utilização por parte das mais variadas organizações.

Se a estupefação quanto ao uso abusivo da figura do consentimento não cercear a nossa incredulidade, é igualmente inconcebível que o Estado, hoje, 3 anos após a entrada em vigor do RGPD, tenha dado conta de que, por exemplo, pelo menos, 1977 freguesias estarão obrigadas a nomear um encarregado de protecção de dados. Subam ou desçam na hierarquia do Estado e imaginem a confusão em que se vive. Três anos volvidos e o Mercado Único Digital Europeu à espreita…

Não pensem, contudo que a confusão é exclusivo do sector público. Quando o foco deriva para dados pessoais sensíveis, nomeadamente, dados de saúde, notícias como por exemplo, «*Proteção de Dados condena clínicas que recusam tratar doentes por falta de assinaturas*[2]», revelam parte do preocupante e actual estado de coisas.

Com efeito, se a protecção de dados pessoais era até há pouco tempo tema desconhecido do grande público, num ápice passou a ser o *olho do furacão*, gerando leque preenchido de atropelos e violações de dados dos seus titulares. E a autoridade nacional de controlo continua amarrada a constrangimentos de índole múltipla, desde orçamentais à falta de recursos, humanos e tecnológicos. Imaginem o que escapa ao *mainstream* mediático.

Enquanto isso, a evolução do digital continua em passo acelerado. O nível de ameaça ao estado de direito democrático acompanha esta desenfreada marcha.

2 Disponível em https://www.dn.pt/lusa/interior/protecao-de-dados-condena-clinicas-que-recusam-tratar-doentes-por-falta-de-assinaturas-10901005.html,

Infelizmente, o tempo do direito e da justiça teimam em não se adaptar. Está assíncrono. O que, se por um lado até poderá induzir-nos a alguma prudência, por outro pode indiciar um factor de preocupação acrescido. Até pelo nível de risco em que coloca a sociedade, no seu todo.

Pensemos na utilização do uso de UAV's; na condução autónoma de veículos; na constante violação das propriedades essenciais da informação gerando supremacias informacionais ilegais a certos Estados; na massificação das redes sociais; na disseminação em *live streaming* de ataques a pessoas; na dispersão de conteúdo mentiroso e propagandístico *online* para desvirtuar o resultado de eleições livres e democráticas; na disseminação de ódio e violência *online*; nas novas ameaças a toda a actividade policial e de segurança do Estado; no controlo e rastreio individual *online* e no registo de crédito social em função disto; entre outras. A profusão destas notícias é de conhecimento geral. A *digitalização* humana está em curso. O ciberespaço, aparentemente, evolui para uma antiutopia.

Neste ensamble, vertiginoso e fulminante, é pois inconcebível que dois anos volvidos após um pedido de fiscalização sucessiva intentado junto do Tribunal constitucional português, por parte de um conjunto de partidos políticos, este Tribunal ainda não se tenha pronunciado quanto à constitucionalidade do acesso aos metadados, dados de tráfego e duração de comunicações por parte dos serviços secretos portugueses. É inconcebível e preocupante pois que, por um lado o serviço de informações da república esteja parado ou a trabalhar à margem da lei ante esta omissão do Tribunal; por outro lado, é inconcebível que este Tribunal, por excelência, de garantia dos direitos e liberdades fundamentais das pessoas, esteja dois anos para aferir da constitucionalidade de uma dada lei.

O que tanto demora a tomada de decisão? Falta de preparação temática dos juízes do Constitucional? Má técnica legislativa? Teimosia política? Falta de ameaças concretas, conhecidas do público, à segurança do Estado? Neste particular dos metadados, sublinho, o delírio é a nota dominante. Até porque, se *o Sistema de Acesso ao Pedido de Dados aos Prestadores dos Serviços de Comunicações Electrónicas (Sapdoc), foi declarado operacional pelo CFSIRP desde Março e está a funcionar*, no outro plano da acção, consta que poderá estar na iminência *um novo chumbo dos juízes,*

uma vez que a questão de fundo - violação do artigo 34º da CRP- manter-se-á [3]. Ora, parece-nos que este delírio, portanto, promete e vai continuar. Novo procedimento, novas discussões, nova lei, mais discussões, novo pedido de fiscalização, novo entorpecimento, novo regresso ao ponto de partida, que recordo, é a nota dominante desde que o poder político criou o *novo regime do Sistema de Informação da República Portuguesa*, em 2015.

Óbice daqui, ameaça dali, risco dacolá, não haverá uma luz de esperança que contrarie o delinear desta *antiutopia*?

A bem de todos nós, mesmo que tenha passado despercebido o *Christchurch Call*[4], julgamos decisivo o apelo à acção. Até porque o momento, o tempo e o espaço a tal nos obrigam. Aqui chegados, impõe-se-nos o sublinhar de parte das notas dos proponentes iniciais. Por um lado, o *envisage* do Presidente francês, o sr. Macron: «"*We need to build this new cyberspace, a free, open and secure Internet, which allows everyone to share, learn, innovate, but which also allows us to uphold our values, protect our citizen and empower them*"»; por outro, o apelo à adesão pluriparticipada, mundial, a cargo da Primeiro-Ministra Neozelandesa, a sra. Ardern: «"*From here, I will work alongside others signed up to the Christchurch Call to bring more partners on board, and develop a range of practical initiatives to ensure the pledge we have made today is delivered*"». Por um *mundo*, terreno e digital, melhor, de todos e para todos.

Por fim, num plano nacional, com especial saudação para a ousadia da proposta, arbitramos da pertinência do Projeto de Lei 1217/XIII[5], apresentado pelo partido Socialista, já apelidado de Carta de Direitos Fundamentais na Era Digital.

A Carta deverá corresponder a *lei de protecção de direitos, liberdades e garantias centrada nas pessoas, consagradora de valores democráticos essenciais contra ameaças que não devem ser ignoradas* procurando ir além de mera *lei compilatória das normas que na ordem jurídica portuguesa consagram (alguns) direitos*, que enuncie *um elenco diversificado e abrangente, que inove, clarifique e valha também*

3 https://www.dn.pt/poder/interior/-necessidade-inquestionavel-fiscais-das-secretas-validam-acesso-a-dados-das-comunicacoes--10935824.html

4 https://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted

5 Disponível em: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=43768

como programa de ação vinculativo dos órgãos de poder, pode ler-se no enunciado programático do Projeto de lei. Deixo aqui um apelo a uma participação contributiva entusiasta por forma a melhorar este esboço inicial de consagração de uma Carta de Direitos Fundamentais na Era Digital.

Resta-me, a final, agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço e pelo trabalho, endereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um reconhecido: Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 24 de Maio de 2019

Nuno Teixeira Castro

CYBERLAW

by CIJIC

DOUTRINA

GESTÃO DE RISCO APLICADA À SEGURANÇA DA INFORMAÇÃO

LUÍSA ALEXANDRA INÁCIO VARANDAS DOS SANTOS [1]

e

MÁRIO RUI MONTEIRO MARQUES [2]

1 Luísa Alexandra Inácio Varandas dos Santos. Correio eletrónico: luisa.santos@tecnico.ulisboa.ptm
[2] Capitão-tenente Mário Rui Monteiro Marques. Correio eletrónico: mario.monteiro.marques@marinha.pt

RESUMO

As sociedades modernas veêm-se, nos dias de hoje, alimentadas por uma quantidade enorme de informação, acrescendo o facto de que numa era digital, essa quantidade de informação é extraordinariamente dinâmica na forma como se produz, como se transforma e como é divulgada.

A informação assume nos dias de hoje, um papel de enorme relevância. O que anteriormente era visto como um ativo valioso apenas pelas forças Militares, passa assim a ter a mesma atenção em contexto Civil na procura da privacidade da informação pessoal dos Cidadãos.

Com o reconhecimento da informação, como um ativo de extremo valor, seja qual for o contexto da sua utilização, passa a existir uma necessidade de a proteger contra ameaças, surgindo assim o conceito de Segurança da Informação com o objetivo de assegurar os princípios e características fundamentais: a confidencialidade, a integridade, a disponibilidade, a autenticidade e não repúdio, e a legitimidade da Informação.

A melhor forma de proteger a informação é conhecer o meio envolvente desta, os fatores internos e externos que a podem influenciar positivamente ou negativamente, que riscos e oportunidades de melhoria existem no seu ciclo de vida e de que forma efetuamos a gestão desses riscos e dessas oportunidades de melhoria, de modo a obter a Segurança da Informação, dentro do contexto em que a mesma se insere.

O presente artigo aborda a "Gestão de Risco aplicada à Segurança da Informação", com uma metodologia baseada na implementação de um processo de gestão de risco segundo a norma *standard* ISO/IEC 31000:2009 - *Risk Management - Principles and guidelines*, integrada com as normas standard em matéria de Gestão Segurança da Informação e Gestão de Serviços de Tecnologias de Informação.

Palavras-Chave: Segurança da informação, Risco, Confidencialidade, Integridade, Disponibilidade, Autenticidade, Legitimidade.

1. INTRODUÇÃO

É em contexto Organizacional que o presente trabalho se pretende focar, onde a simples necessidade de gestão de dados de processos de negócio, passou a uma imprescindível necessidade de transformar a informação dos processos de negócio em conhecimento valioso para a tomada de decisões estratégicas das Organizações.

Esta crescente necessidade Organizacional, de gerir a informação de processos de negócio de modo a produzir conhecimento estratégico, recorre às Tecnologias e Sistemas de Informação, assumindo estas o seu lugar de relevância nas Organizações. Por este motivo, as Tecnologias e Sistemas de Informação têm sido particularmente beneficiadas em investimentos das Organizações respetivas, procurando uma evolução Tecnológica continua e apta a responder com eficiência aos desafios de negócio em que determinada Organização se insere. Tendo sido este o fator de sucesso em mercados de enorme concorrência. Conhecer a Organização, conhecer os produtos e serviços que a mesma produz, conhecer os seus Clientes, Fornecedores e partes interessadas, conhecer a informação Organizacional e protege-la de ameaças, é um fator de sucesso e até mesmo de sobrevivência em mercados de muita concorrência, ou mercados extremamente regulados e legislados particularmente em matéria de informação sensível e secreta, como é o caso por exemplo do setor da Saúde e do setor Judicial!

Temos assistido, não só ao crescimento dos Sistemas de Informação Organizacionais, mas também, a um aumento de interações entre vários Sistemas de Informação, que facilmente comunicam entre si, permitindo obter, tratar, armazenar e divulgar informação de uma forma integrada e potencialmente útil à estratégia das Organizações, onde estão inseridos.

A legislação que tem surgido nas últimas décadas, quer a nível nacional quer a nível europeu, tem-se esforçado por acompanhar a preocupação da Segurança da Informação, com o foco na Segurança das Redes e da Informação, Interoperabilidade Digital e Privacidade de Dados Pessoais, respetivamente: RNID - Regulamento Nacional de Interoperabilidade Digital, Diretiva UE 2016/1148 e Regulamento (UE) 2016/679 [6], [7] e [8].

Ainda assim, pese embora tenha crescido a preocupação da União Europeia e dos seus Estados Membros em legislar sobre Segurança da Informação em matéria de redes, sistemas de informação e dados pessoais, apelando a uma gestão do risco e a potenciais ameaças, o facto é, que a lei tem sido omissa na metodologia que as Organizações devem adotar para implementação de processos de gestão de risco, deixando a cargo das mesmas a adoção de processos de cerificação voluntários que possam contribuir para o cumprimento da legislação em vigor na prevenção contra ameaças. Neste sentido, a maior parte das Organizações tem recorrido às normas *standard* ISO "Internacional Organization for Standardization", Organização internacional não-governamental independente, com sede em Genebra, que desenvolve padrões de normalização para o âmbito Organizacional, tais como: Gestão de Segurança da Informação, Gestão de Serviços de Tecnologias de Informação, Gestão de Risco, entre outros. O presente trabalho tendo como foco a "Gestão de Risco aplicado á Segurança da Informação", pretende assim demonstrar a aplicabilidade prática da adoção de um processo de Gestão de Risco segundo a norma *standard* ISO/IEC 31000:2009 – "*Risk Management - Principles and guidelines*" (**Figura 1**), acompanhada das normas standard em matéria de Gestão de Segurança da informação e Gestão de Serviços de Tecnologias de Informação.

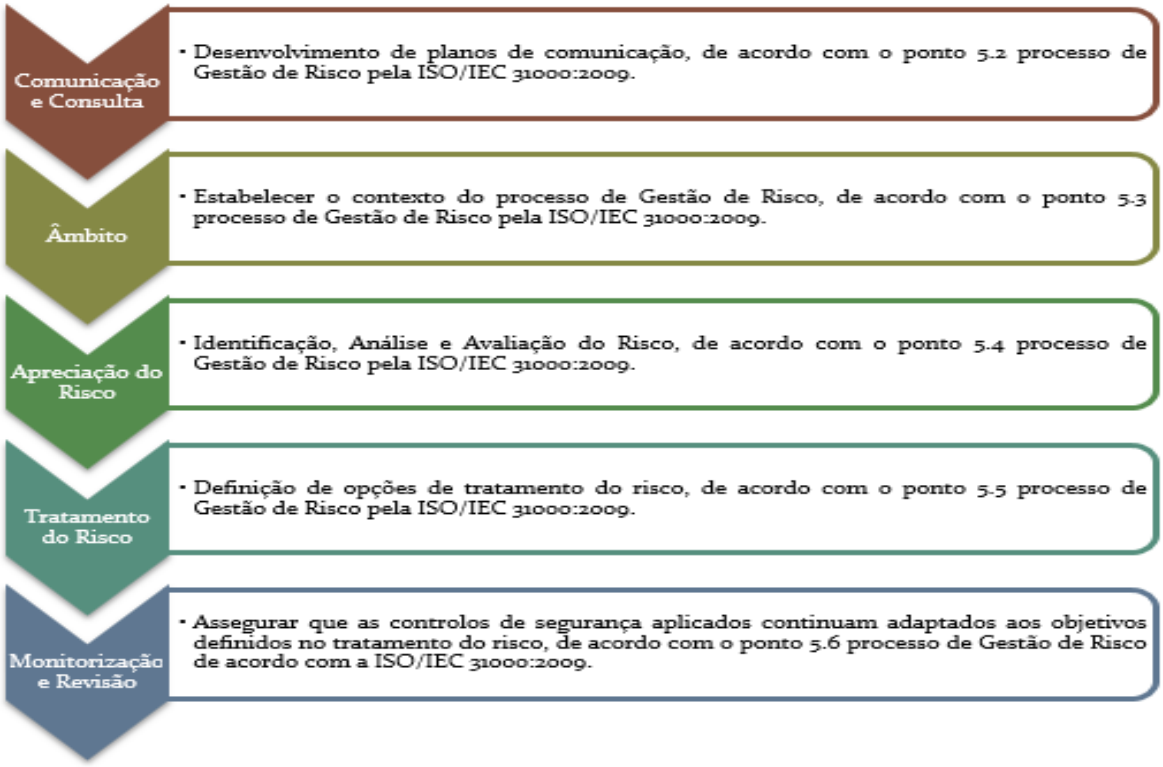

Figura 1 – Fases de processo de Gestão de Risco pela ISO/IEC 31000:2009 - Risk Management - Principles and guidelines [5]

2. PROCESSO DE GESTÃO DE RISCO APLICADO À SEGURANÇA DA INFORMAÇÃO

As Organizações têm várias componentes que não apenas a tecnológica e o negócio, que carecem de análise na implementação de um Processo de Gestão de Risco aplicado à Segurança da informação adiante designado por **PGRSI**, entre elas, temos a considerar, a componente humana, ou seja, os Colaboradores de determinada Organização, os seus Fornecedores e Partes Interessadas.

Todas as componentes envolvidas na implementação de um Processo de Gestão de Risco aplicado á Segurança da informação em determinada Organização, requerem especial preocupação relativamente a vulnerabilidades que as mesmas possam ter, face a potenciais ameaças, ou seja, de que modo essas componentes Organizacionais estão realmente protegidas no âmbito da Segurança da Informação, reduzindo e minimizando o impacto de uma ameaça a determinada Organização.

Existe assim a necessidade da Organização analisar todas as condicionantes internas e externas que possam representar riscos significativos para a Segurança da Informação da Organização, mais especificamente que coloquem em causa os princípios da Segurança da Informação de determinada Organização [1]:

- **Confidencialidade** - assegurar que apenas quem está autorizado é que pode aceder à informação. Esta característica depende de um procedimento interno de classificação de informação, definido pela Organização, identificando que informação é confidencial, secreta, publica, interna, ou, outro tipo de informação, definindo por cada tipo de classificação de informação, quem pode aceder e, de que modo pode aceder ou divulgar informação [1], [2], [3] e [4].

- **Integridade** - assegurar que a informação e os seus métodos são completos. Isto significa que independentemente dos canais e formas onde a informação possa ser tratada e divulgada, a mesma, nunca perde o seu valor conceptual nem é adulterada. Esta situação depende de um procedimento interno de definição e controlo de versões de informação que possa ser produzida sobre a mesma origem, definido pela Organização, identificando todas as versões que foram produzidas sobre a mesma informação, datas e autores de versões

produzidas, bem como, identificação de que informação adicional acrescida, ou, que informação foi retirada da inicial [1], [2], [3] e [4].

- **Disponibilidade** - assegurar que os utilizadores autorizados têm acesso à informação e aos seus ativos associados sempre que necessitem. Obviamente que este tipo de característica tem de levar em conta o tipo de informação e a quem deve ser disponibilizada, dependendo da sua classificação [1], [2], [3] e [4].

- **Autenticidade e não repúdio/desconhecimento** - assegurar a fiabilidade das transações e o intercâmbio de informação entre organizações e colaboradores. Esta característica pode ser garantida através de utilização de mecanismos de backup de logs (registos) de dados de acesso e alteração da informação [1], [2], [3] e [4].

- **Legitimidade** - garantir que o tratamento da informação cumpre com as leis e regulamento do sector (área de negócio) a que se aplica [1], [2], [3] e [4].

É também importante destacar outros princípios que a Segurança da Informação tem implícitos, pese embora não sejam aqueles que definem as suas características fundamentais, ainda assim também estes carecem de preocupação face a possíveis riscos a que possam estar sujeitos, nomeadamente:

- A proteção dos dados de carácter pessoal e a privacidade das pessoas;

- A proteção dos direitos de propriedade intelectual e industrial;

- O estabelecimento de um sistema de classificação da informação com o objetivo de proteger melhor os ativos críticos da organização;

- A salvaguarda dos registos da organização.

É através da implementação de um **PGRSI**, que a Organização consegue avaliar o impacto dos riscos que podem pôr em causa os princípios e características fundamentais da Segurança da Informação, antecipando ações corretivas aos riscos detetados.

3. PGRSI - COMUNICAÇÃO E CONSULTA

Esta fase engloba todas as outras do **PGRSI** (**Figura 1**), a Organização deve comunicar com todas as partes interessadas, Colaboradores, Clientes, Fornecedores, etc…, desenvolvendo planos de comunicação e consulta, abordando as questões relacionadas com o risco, causas e consequências do mesmo e formas de tratar o risco, na Organização.

Na prática esta fase é alimentada pelas fases seguintes que serão demonstradas, sendo que nesta fase, abrangendo todo o **PGRSI**, podem ser consultadas as partes interessadas da Organização de modo a definir critérios de risco e avaliação de risco, para os riscos identificados e comunicados. Assim, devemos olhar para esta fase, como um comportamento da Organização reagindo a eventos decorrentes da implementação do **PGRSI** que devem ser prontamente comunicados e consultados pelas partes interessadas de modo a contribuir para a melhoria contínua do **PGRSI**.

4. PGRSI - ÂMBITO

O âmbito de aplicação do **PGRSI**, resulta da identificação correta de todas as componentes Organizacionais que produzem, acedem, tratam e disponibilizam informação, no sentido de identificar onde, como e com que probabilidade se podem concretizar riscos numa Organização. Deste modo, pode ser definido o âmbito do **PGRSI** da seguinte forma:

- **RECURSOS INTERNOS** – Recursos humanos internos á Organização tais como: Auditores Internos, Juristas internos, Utilizadores Internos, Colaboradores Internos em geral, etc.
- **RECURSOS EXTERNOS** – Recursos humanos externos á Organização Auditores Externos, Consultores, Prestadores de Serviço, Utilizadores Externos, Colaboradores Externos em geral, etc
- **SERVIÇOS DE TECNOLOGIAS DE INFORMAÇÃO** – Conjunto de Sistemas de Informação que dão suporte ao negócio numa Organização, por exemplo soluções de *Business Intelligence* (processos de tratamento de dados de larga escala), soluções de Sistemas de Informação Integrados de Processos de Negócio da Organização, etc.
- **PARTES INTERESSADAS À ORGANIZAÇÃO** – Fornecedores internos e externos, Clientes, Negócio.
- **DOCUMENTOS CONTROLADOS E ACORDOS DOCUMENTADOS** – Acordos de Níveis de Qualidade e Disponibilidade de Serviço, Políticas e Regulamentos Organizacionais, Legislação, Códigos de Conduta, e Planos (Contingência, Continuidade de Negócio, Plano de Tratamento do Risco, entre outros).
- **SOFTWARE** – Sistemas Operativos, Aplicações e Bases de Dados.
- **DISPOSITIVOS** – Computadores, Monitores, Discos, Smartphones, Tablets, etc.
- **COMUNICAÇÕES** – Circuitos Internet, Circuitos de Voz, etc.
- **SERVIDORES** – Centralização de fornecimento de serviços e protocolos de rede.
- **ARMAZENAMENTO DE DADOS** – Arquiteturas de Armazenamento de dados.
- **INFRAESTRUTURA DE REDE** – Redes de dados Locais e Virtuais.

Estamos assim perante o âmbito de aplicação do **PGRSI**, que comporta toda a informação, nas suas formas, suportes e canais de circulação, assumidos no seu ciclo de vida, dentro de uma Organização e de todas as suas partes interessadas. Reconhecendo que o âmbito de aplicação do **PGRSI** nomeadamente: a Organização em si, Fornecedores, Clientes, Mercado, Legislação e Regulação, evoluem ao longo do tempo, o **PGRSI**, deve permitir avaliar aquilo que hoje constitui uma ameaça, mas que amanhã pode não constituir, passando a representar uma oportunidade.

5. PGRSI - APRECIAÇÃO DO RISCO

A fase de Apreciação do Risco resulta de um processo global de identificação, análise e avaliação do mesmo, passamos assim a demonstrar de uma forma integrada estas fases, tendo em conta o âmbito do **PGRSI**. Importa antes de tudo distinguir o que são ameaças e o que são vulnerabilidades:

- **AMEAÇA**, representa um possível ataque interno ou externo a determinado alvo, com intenção de provocar danos totais ou parciais nesse alvo.
- **VULNERABILIDADE**, representa alguma fragilidade de determinado alvo, que possa ser explorada por uma ameaça de modo a provocar maior impacto num determinado ataque, ou seja, conteúdos não protegidos, ou, com reduzida proteção, ou, com proteção desatualizada e que não acompanham as ameaças atuais.

5.1. Identificação do risco

5.1.1. Inventário de ativos

Procede-se á identificação dos ativos a proteger e dependências entre si dentro do âmbito do **PGRSI**, através da realização de um inventário de Ativos, em que um Ativo é um item que suporta informação, dentro do âmbito do **PGRSI**, com valor para a Organização e dos quais dependem a realização de atividades de Serviços de Tecnologias de Informação como, por exemplo: Servidores, Computadores, *Smartphones*, Impressoras, Discos e Unidades de Armazenamento, Circuitos de Comunicação, etc.

O inventário de Ativos deve permitir valorizá-los em função do seu impacto para a Organização, tendo em conta, incidentes relacionados com os princípios da Segurança da informação, de confidencialidade, de integridade, de disponibilidade, de autenticidade e não repúdio, e de legitimidade da informação. Desta forma deve-se inventariar os Ativos da seguinte forma:

- ✓ Designação do Ativo;
- ✓ Dependentes diretos do Ativo;
- ✓ Localização do Ativo;
- ✓ O dono ou responsável pela sua utilização do Ativo;
- ✓ Os serviços ou processos nos quais o Ativo está envolvido.

5.1.2. Matriz de impacto

Define-se uma Matriz de Níveis de Impacto e de Linhas Orientadoras para a análise de impacto, de modo a quantificá-lo face á concretização de uma ameaça, através da definição de níveis de impacto por determinados valores definidos para linhas orientadoras.

Estas linhas orientadoras podem levar em conta os contributos das partes interessadas, conforme previsto na fase de Comunicação e Consulta do **PGRSI**. Propõe-se a título de exemplo as seguintes dimensões para a elaboração da Matriz:

a. **Níveis de Impacto -** Estabelecemos os níveis de impacto de 1 a 5, para os diferentes valores de cada linha orientadora (b.) de análise de impacto de concretização da ameaça, com o seguinte critério:

- ✓ **Nível 1** Sem Impacto nos serviços prestados;
- ✓ **Nível 2** Impacto reduzido nos serviços prestados;
- ✓ **Nível 3** Impacto significativo nos serviços prestados;
- ✓ **Nível 4** Impacto grave nos serviços prestados;
- ✓ **Nível 5** Ameaça à sobrevivência do Negócio.

b. **Linhas Orientadoras -** Estabelecemos as linhas orientadoras de análise de impacto de concretização da ameaça, do seguinte modo:

- ✓ **Perdas Financeiras** - Perda direta de clientes ou quota de mercado, custos de oportunidade, perda de vantagens competitivas e/ou custos de recuperação.
- ✓ **Esforço de Operações** - Incremento dos esforços de produção, esforços operacionais, esforços associados à contratação de RH adicionais e/ou de recuperação de imagem.
- ✓ **Reputação e Imagem** - Perda de confiança dos clientes, público em geral, partes interessadas, entidades reguladoras, entidades de supervisão e/ou colaboradores.
- ✓ **Legais/Regulamentares** - Sujeição a potenciais investigações, multas ou penalidades por parte de entidades reguladoras/governamentais, sanções contratuais e/ ou processos em tribunal.
- ✓ **Envolvimento da Gestão de Topo da Organização** - Envolve diretamente a Gestão de Topo influenciando o processo de tomada de decisão,

seja a nível estratégico, de investimentos e/ou conceção e desenvolvimento de novos serviços.

c. **Matriz de Limites de Impacto por Valores de Linhas Orientadoras para a avaliação de impacto -** Com base nos níveis de impacto definidos em (a.) relacionados com as linhas orientadoras de análise de impacto definidas em (b.), estabelece-se a seguinte Matriz de limites orientadores de avaliação de impacto (**Figura 2**):

a. Níveis de Impacto	b. Linhas Orientadoras				
IMPACTO	**PERDAS FINANCEIRAS**	**ESFORÇO DE OPERAÇÕES**	**REPUTAÇÃO E IMAGEM**	**LEGAIS E REGULAMENTARES**	**EMVOLVIMENTO DA GESTÃO DE TOPO DA ORGANIZAÇÃO**
1 Sem **Impacto nos serviços prestados**	Perdas até X.000,00€	Sem impacto significativo no esforço operacional	Afeta negativamente as relações com outras partes da Organização. Sem impacto nos meios de comunicação.	Sem impacto significativo no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Resolução de incidentes ao nível das equipas técnicas, o serviço afetado não é estratégico para a Organização.
2 **Impacto reduzido nos serviços prestados**	Perdas até XX.000,00€	Impacto reduzido no esforço operacional	Afeta negativamente as relações com o publico e com outras organizações no meio. Atenção pontual nos meios de comunicação, mas sem por em causa a imagem da Organização.	Impacto reduzido no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Resolução de incidentes ao nível das equipas técnicas, com necessidade de esclarecimentos dos diretores de primeira linha, o serviço afetado não é estratégico para a Organização.
3 **Impacto significativo nos serviços prestados**	Perdas até XXX.000,00€	Impacto significativo no esforço operacional (sobrecarga de recursos).	Afeta negativamente as relações com o publico e com outras Organizações. Atenção adversa nos meios de comunicação, mas sem por em causa a imagem da Organização.	Impacto significativo no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Envolvimento direto dos diretores de primeira linha na resolução de incidentes, a Gestão de Topo da Organização é notificada, o serviço afetado não é estratégico para a Organização.
4 **Impacto grave nos serviços prestados**	Perdas até X.000.000,00€	Grande impacto no esforço operacional, alocação de horas extra aos recursos.	Publicidade Negativa passa nos meios de comunicação, suscetível de colocar em causa a imagem da Organização.	Grande impacto no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Requer decisão e gestão pontuais por parte da Gestão de Topo da Organização, o serviço afetado é

					estratégico para a Organização.
5 **Ameaça à sobrevivência do Negócio / Prestação de Serviço**	Perdas superiores a X.000.000,00€ ou perdas suficientes para impedir a continuidade do negócio	Impacto Catastrófico no esforço operacional (para além de alocação de horas extra aos recursos, existe a necessidade de suspender atividades diárias).	Publicidade Negativa passa nos meios de comunicação com grande repercussão, colocando em causa a imagem da Organização.	Impacto catastrófico no cumprimento de contratos, acordos, regulamentações e leis em vigor.	Requer envolvimento ativo da Gestão de Topo da Organização, o serviço afetado é estratégico para a Organização.

Figura 2 – Matriz de Limites de Impacto por Valores de Linhas Orientadoras para a avaliação de impacto (a Matriz é puramente exemplificativa podendo ser gerada outra qualquer Matriz ao critério do Responsável pela implementação de um PGRSI em determinada Organização e Contexto Organizacional)

5.1.3. Avaliação do impacto sobre os ativos

É necessário avaliar para cada ativo, de acordo com a Matriz de limites orientadores de avaliação de impacto (**Figura 2**), na fase em que não existem medidas aplicadas, ou seja, sem controlos de segurança da informação aplicados, o impacto que terão caso se verifiquem incidentes de segurança da informação relacionados com a confidencialidade, a integridade, a disponibilidade, a autenticidade e não repúdio, e a legitimidade da informação. O valor máximo da matriz associada a cada ativo dar-nos-á o valor do mesmo; no entanto, se outros ativos dependem dele, o valor do ativo que estamos a analisar passará a ser o valor máximo dos ativos dependentes deste.

A título de exemplo, podemos olhar para os seguintes ativos um Servidor de Comunicações de Voz de uma Organização e um Servidor Web de suporte a um Site Institucional dessa mesma Organização, se avaliarmos o seu impacto de acordo com a Matriz de impacto por ativo (**Figura 3**), tendo em conta a existência de incidentes se segurança da

informação, que coloquem em causa a confidencialidade, a integridade, a disponibilidade, a autenticidade e não repúdio, e a legitimidade da informação, teríamos a seguinte escala de ponderação:

Incidente	Escala	Nível Impacto apurado de acordo com linhas orientadoras (Figura 2) Ativo Servidor Comunicações	Nível Impacto apurado de acordo com linhas orientadoras (Figura 2) Ativo Servidor Web
Disponibilidade	Falha na disponibilidade até 15 minutos	1	1
	Falha na disponibilidade até 3 horas	2	1
	Falha na disponibilidade até 1 dia	3	2
	Destruição Parcial de Informação	4	3
	Destruição Total de Informação	5	4
Integridade	Modificação não publicada	1	1
	Modificação sem controlo de versões	2	1
	Modificação não autorizada	3	2
	Perda parcial de histórico de versões	4	3
	Perda total de histórico de versões	5	4
Confidencialidade	Informação não classificada	1	1
	Informação confidencial acedida por pessoa interna não autorizada	2	1
	Informação confidencial acedida por pessoa externa não autorizada	3	2

	Divulgação interna de informação confidencial	4	3
	Divulgação externa de informação confidencial	5	4
Autenticidade e Não Repúdio	Informação sem fonte de autenticidade	1	1
	Alteração por negligência de autenticidade da Informação	2	1
	Alteração propositada de autenticidade da Informação	3	2
	Divulgação interna de informação sem autenticidade	4	3
	Divulgação externa de informação sem autenticidade	5	4
Legitimidade	Evidencia de não conformidade com regulamentos internos	1	1
	Evidencia de não conformidade normativa ou regulamentar	2	1
	Evidencia de não conformidade legal de acordo com legislação aplicada à área de negocio da Organização	3	2
	Dados pessoais acedidos, ou, sobre alvo de tratamento sem autorização dos titulares	4	3
	Dados Sensíveis acedidos, ou, sobre alvo de tratamento sem autorização dos titulares	5	4

Figura 3 – Matriz de impacto por Ativo (a Matriz é puramente exemplificativa podendo ser gerada outra qualquer Matriz ao critério do Responsável pela implementação de um PGRSI em determinada Organização e Contexto Organizacional)

Podemos assim verificar que o valor máximo da matriz associada a cada ativo dar-nos-á o valor de cada um dos ativos em análise, assim poderemos dizer, ainda na fase em que não existem medidas aplicadas, ou seja, sem controlos de segurança da informação, que o valor de impacto sobre o ativo Servidor de Comunicações de Voz de uma Organização é 5 (Ameaça à sobrevivência do Negócio de acordo com Figura 2) e o valor de impacto sobre o ativo Servidor Web de suporte a Site Institucional é 4 (Impacto grave nos serviços prestados de acordo com **Figura 2**), máximos valores assumidos por cada um dos ativos na Matriz de impacto por ativo (**Figura 3**).

5.2. Análise do risco

5.2.1. Identificação das ameaças a que estão expostos os ativos

Identificam-se, as ameaças às quais, se considera, que possam estar expostos os ativos por exemplo: desastres naturais (sismos, terramotos, etc), inundações, incêndio, falta de recursos humanos ou equipa insuficiente, acidentes de trabalho, manipulação de informação e cópias de informação, corrupção ou má configuração de *software*, abuso de direitos de perfil de administração de rede informática, acesso físico ou logico não autorizado a instalações e áreas condicionadas, etc…

Para cada uma das ameaças será necessário valorizar, tanto o antes como o depois da aplicação de medidas de segurança, o valor de frequência da mesma.

O valor da ameaça de cada ativo pode ser medido pela implementação de um processo de gestão de incidentes de segurança da informação [3] e [4], obtendo o número total de incidentes com a causa em determinada ameaça sobre um ativo, em determinado período. Para este trabalho, vamos hipoteticamente referenciar os seguintes valores:

- ✓ **Baixa (B):** Verificado pelo menos um Incidente de determinada ameaça sobre determinado ativo num período > 12 meses;
- ✓ **Média (M):** 6 meses < Verificado pelo menos um Incidente de determinada ameaça sobre determinado ativo num período < 12 meses;
- ✓ **Alta (A):** Verificado pelo menos um Incidente de determinada ameaça sobre determinado ativo num período < 6 meses ou menos.

Uma vez valorizadas as ameaças para cada um dos ativos, caso um deles seja alvo de várias ameaças, o valor de ameaça do ativo será o maior valor de todas as suas ameaças.

5.2.2. Identificação das vulnerabilidades a que estão expostos os ativos e a sua relação com as ameaças

Para cada ativo devem-se identificar, sobretudo em função de cada ameaça, as vulnerabilidades que possam favorecer a sua ação, indicando a probabilidade de que possa ocorrer o pior cenário possível, por exemplo: armazenamento de informação não protegido, baixas de pessoal, controlo de recrutamento inadequado, falha de fornecimento de energia, ausência de plano de incêndio, controlo de acessos de rede inadequado, ausência de controlo de licenciamento de software, ausência de formação profissional dos recursos, ausência de politicas/procedimentos/normas etc…

O valor da vulnerabilidade de cada ativo pode ser medido pela implementação de um processo de gestão de incidentes de segurança da informação [3] e [4], obtendo a percentagem da vulnerabilidade através do número de incidentes com a causa em determinada vulnerabilidade de um ativo, em determinado período, sobre o número total de incidentes de segurança que esse ativo teve com a mesma vulnerabilidade em determinado período. Para este trabalho, vamos hipoteticamente referenciar os seguintes valores:

- ✓ **Baixa (B):** Probabilidade de ocorrência de determinada vulnerabilidade sobre determinado ativo no espaço de um ano < 33%;

- ✓ **Média (M):** 33% < Probabilidade de ocorrência no espaço de um ano < 66%;

- ✓ **Alta (A):** Probabilidade de ocorrência no espaço de um ano > 66%.

Uma vez valorizadas as vulnerabilidades para cada um dos ativos, caso um deles tenha várias vulnerabilidades, o valor da vulnerabilidade do ativo será o maior valor de todas as suas vulnerabilidades.

5.3. Avaliação do risco

5.3.1. Cálculo do risco intrínseco

O Risco Intrínseco, é o risco sem a aplicação de qualquer tipo de medidas de segurança, ou seja, é o risco que os ativos têm por si, em função das ameaças e vulnerabilidades que lhes são aplicáveis.

Caso se analisem os valores de cada ativo, o seu valor de ameaça e o seu valor de vulnerabilidade (**Figura 4**), obteremos o Risco Intrínseco de cada ativo.

	Ameaça	Baixa			Média			Alta		
	Vulnerabilidade	B	M	A	B	M	A	B	M	A
Valor do Impacto sobre o Ativo segundo matriz **Figura 3**	0	0	1	2	0	1	2	0	1	2
	1	1	2	3	1	2	3	1	2	3
	2	2	3	4	2	3	4	2	3	4
	3	3	4	5	3	4	5	3	4	5
	4 (valor Ativo SW)	4	5	6	4	5	6	4	5	**6**
	5 (valor Ativo SCV)	5	6	7	5	6	**7**	5	6	7

Figura 4 – Exemplo de Matriz de Risco Intrínseco (a Matriz é puramente exemplificativa podendo ser gerada outra qualquer Matriz ao critério do Responsável pela implementação de um PGRSI em determinada Organização e Contexto Organizacional)

Nos exemplos dos ativos dados no ponto 5.1.3. - Avaliação do Impacto sobre os Ativos, o valor do Ativo Servidor de Comunicações de Voz é 5 e o valor do Ativo Servidor Web de suporte a Site Institucional é 4 (**Figura 3**), estamos tipicamente nas duas últimas linhas da Matriz de Risco Intrínseco (**Figura 4**), agora imaginemos o seguinte:

Os Ativos, Servidores, foram alvo de uma auditoria de segurança no ano de 2018 e verificou-se que:

- Tanto o Servidor de Comunicação de Voz (SCV) como o Servidor Web (SW) não tinham protocolos de segurança adequados, tendo sido alvos de vários ataques. No caso do SCV foi atacado em espaços temporais de 7 em 7

meses (Ameaça Média ponto 5.2.1.), já o SW foi atacado em espaços temporais de 1 em 1 meses (Ameaça Alta ponto 5.2.1.).

- Enquanto não forem aplicados protocolos de segurança nestes Servidores existe uma probabilidade de 100 % de ocorrência no período de um ano de novos ataques para ambos (Vulnerabilidade Alta de ambos os Servidores ponto 5.2.2.).

Assim, segundo a Matriz de Cálculo do Risco Intrínseco (**Figura 4**), temos o valor Risco Intrínseco = **6** para o Ativo SW e Risco Intrínseco = **7** para o Ativo SCV.

Deve ser elaborado um relatório do Risco Intrínseco, para todos os ativos do **PGRSI**, em que o Risco Total Intrínseco será o resultado de uma média aritmética simples dos valores de risco intrínseco dos ativos (dividir a soma dos riscos intrínsecos pelo número de ativos). O relatório deve ser divulgado á Gestão de Topo da Organização.

5.3.2. Definição do risco aceitável

A Gestão de Topo da Organização define o nível de riscos que está disposta a assumir, denominado "limite de risco", sendo necessária a gestão do risco dos ativos cujo valor de risco intrínseco seja superior a esse valor.

Imaginemos por exemplo que a Gestão de Topo defina o Risco Aceitável = 3, observamos que os ativos analisados no ponto 5.3.1. (**Figura 4**) com um Risco Intrínseco superior ao Risco Aceitável pela Gestão de Topo, assim, ambos os Ativos têm de ser alvo de medidas de segurança que permitam reduzir o Risco Intrínseco apurado até ao nível aceitável definido pela Gestão de Topo.

O limite de risco, ou Risco Aceitável, resulta do equilíbrio entre as medidas de segurança da informação a implementar e o impacto dessas. Se não se poderem cumprir essas medidas de segurança, deve-se, ou modificar de novo o limite de Risco Aceitável pela Gestão de Topo, ou, aplicar novas medidas de segurança da informação. Será uma decisão da Gestão de Topo da Organização!

O limite de risco do serviço é definido e revisto num determinado período temporal e aprovado diretamente pela Gestão de Topo, mesmo que se mantenha o nível do período anterior.

Para aqueles riscos que ultrapassam o limite de risco aceitável, realiza-se um procedimento de Tratamento de Riscos, de acordo com a fase descrita no ponto seguinte.

6. PGRSI - TRATAMENTO DO RISCO

A fase de tratamento de risco é levada a cabo aquando de uma primeira avaliação, assim que conhecido o Risco Aceitável pela Gestão de Topo e finalizada a análise do Risco Intrínseco (ponto 5.3.) ao qual estão sujeitos os ativos incluídos no respetivo âmbito do **PGRSI**, ou, sempre que se realize uma análise de riscos na organização.

Nesta fase são definidas as opções de tratamento do Risco Intrínseco (sem aplicação de medidas de segurança) face ao Risco Aceitável (limite de risco aceitável pela Gestão de Topo), e posteriormente apurado o Risco Residual, ou seja, o Risco apurado após aplicação de medidas de segurança sobre os Ativos.

Caso o Risco Residual não seja ainda aceitável, deve ser efetuado novo tratamento de risco, com aplicação de novas medidas de segurança que permitam uma das seguintes ações: evitar, assumir explorando oportunidades, remover, alterar, partilhar, ou, reter o risco [5].

A seleção de opções de tratamento do risco, ou seja, de aplicação de medidas de segurança, implica sempre a que a Organização faça uma relação de custo face ao benefício, relativamente aos esforços financeiros e operacionais levados em conta para a implementação de medidas de segurança para tratamento de determinado risco.

Deve ser definido um Plano de Tratamento de Risco de modo a documentar todas as opções identificadas para o tratamento dos riscos, dando a conhecer esse plano e o Risco Residual apurado á Gestão de Topo e às partes interessadas.

O Risco Residual assumido pela Organização, especificamente pela Gestão de Topo, deve ser alvo de monitorização, revisão e tratamento posterior, de acordo com a procura da melhoria contínua do próprio **PGRSI**.

6.1. Medidas de segurança da informação

As medidas de segurança a aplicar sobre os Ativos, de modo a obter o Risco Residual, devem referenciar os seguintes parâmetros:

- ✓ O custo de implementação de cada medida de segurança;
- ✓ O tipo de medida de segurança (Jurídica, Tecnológica, Gestão, etc);

- ✓ O tipo de proteção (evitar, detetar, reduzir o impacto, recuperar, redução da ameaça, transferir o risco, explorar e redução de vulnerabilidade);
- ✓ O seu estado (em estudo, em implementação, aplicada, revista);
- ✓ O controlo legal e normativo, à qual faz referência.

No caso de existirem condicionamentos de aplicação das medidas de segurança, devem ser indicados quais os fatores que condicionaram a sua ausência de aplicação.

6.2. Cálculo risco residual

Implementadas as medidas de segurança por ativo com o Risco Intrínseco superior ao Risco Aceitável, calculamos o Risco Residual, ou seja, o nível de risco resultante após implementação das medidas aplicáveis de segurança da informação, documentando esta operação no documento de aplicabilidade SoA (*Statement of Applicability*) [5].

No SoA relacionam-se todos os controlos de segurança, tanto os que serão implementados como os que não serão implementados, para os não implementados dever-se-á justificar a não implementação, de modo a reduzir a frequência de ocorrência das ameaças avaliadas na análise de riscos, e as ações previstas no Plano de Tratamento de Riscos atual. Por tudo isto, o Risco Residual é o risco a ser assumido pela Gestão de Topo.

Serão assim, calculados de novo os valores de risco dos ativos, após nova revisão dos valores das ameaças e das vulnerabilidades de cada ativo, ou seja, após aplicação de controlos de segurança.

O Risco Residual apurado deve ser detalhado, tanto por ativo como por serviço, com a finalidade de conhecer as áreas em que será necessário dar prioridade na implementação de novos controlos de segurança no Plano de Tratamento de Riscos.

6.3. Aceitação pela gestão de topo

A Gestão de Topo, considera que, tanto o custo das medidas a implementar como o Risco Residual resultante, são aceitáveis, em função dos objetivos estratégicos e de segurança da Organização, considerados em cada período definido, desta forma a Gestão de Topo deve aprovar a conformidade do documento de aplicabilidade SoA e ao relatório de Risco Residual para proceder à sua implementação.

Em caso de rejeição, a Gestão de Topo deverá expor os seus motivos, procedendo-se assim a uma nova seleção de controlos e contramedidas de segurança, para posteriormente realizar um novo cálculo do Risco Residual e elaborar um novo relatório de Risco Residual que seguirá o mesmo processo até aqui exemplificado, até à sua aceitação por parte da Gestão de Topo.

6.4. Plano tratamento de riscos

Estabelece-se no Plano de Tratamento de Riscos, as ações que a Organização vai realizar para implementar os controlos de segurança selecionados no documento de aplicabilidade (SoA - *Statement of Applicability*, documento de seleção de controlos), levando em conta:

- ✓ Calendário de implementação, definindo metas e datas para a sua realização;
- ✓ Priorizar ações com base nos resultados da análise de risco;
- ✓ Atribuir responsabilidades, antes da implementação dos controlos, identificar os responsáveis por assegurar a correta implementação de cada um dos controlos de segurança;
- ✓ Planear a aquisição ou disponibilidade dos recursos necessários.

O Plano de Tratamento de Riscos deve também ser aprovado pela Gestão de Topo.

7. PGRSI - MONITORIZAÇÃO E REVISÃO

O **PGRSI** deve permitir identificar novas ameaças ao longo do tempo, podemos assim assegurar que o **PGRSI** desempenha um papel preponderante na atualização, revisão e seguimento das ameaças, vulnerabilidades, riscos e controlos de segurança da informação aplicados sobre os Ativos do âmbito do **PGRSI**.

Esta fase do **PGRSI** é também ela, á semelhança da fase Comunicação e Consulta, transversal a todas as fases do **PGRSI**, e consiste em verificar de modo regular o próprio **PGRSI**, sendo que para isso deve a Gestão de Topo definir o período temporal em que a monitorização e a revisão do **PGRSI** são efetuadas.

A monitorização e revisão do **PGRSI** asseguram que os controlos de segurança aplicados continuam adaptados aos objetivos definidos no tratamento do risco, face a possíveis alterações internas e externas á Organização, perseguindo assim a melhoria contínua do **PGRSI**.

8.CONCLUSÕES

Numa perspetiva Organizacional os processos de gestão de risco sempre foram, de certa forma de modo voluntário e nunca como um pressuposto de obrigação legal, aplicados ao sucesso de uma Organização, avaliando os contextos sociais, políticos e económicos, em que essa se insere e as potenciais ameaças ao sucesso do seu negócio. O conceito Gestão de Risco tem sido assim, aplicado nos mais variadíssimos contextos Organizacionais, Gestão de Risco em Projetos, Gestão de Risco Empresarial e Gestão de Risco Financeiro, entre outos.

O que é curioso é que as doutrinas de Gestão de Risco, no momento em que surgiram num contexto Organizacional, não acentuavam o seu foco em preocupações tais como: a Informação como um ativo vital numa Organização, a era das Tecnologias e Sistemas de Informação, a era da procura da confidencialidade, da integridade, da disponibilidade, da autenticidade e não repúdio, e da legitimidade da informação, como fator de relevância numa avaliação de impacto de risco Organizacional.

É a partir do momento em que se reconhecem todas estas preocupações, numa era totalmente digital, que a informação passa a ser um ativo demasiado valioso e protegido pelas Organizações. Esta preocupação é acompanhada por legislação e normas *standard*, promovendo a implementação de processos Organizacionais num contexto de Segurança da Informação.

Com o contexto Segurança da Informação, surge assim a definição da metodologia de Gestão de Risco aplicada à Segurança da Informação, pese embora o facto da sua implementação continuar a ser visto sob com uma perspetiva voluntária das Organizações e não obrigatória.

Não existe nenhum sistema 100% seguro, mesmo com a adoção de processos de cerificação voluntários que possam contribuir para o cumprimento da legislação em vigor na prevenção contra ameaças, no entanto cada vez mais se torna evidente que os processos de gestão de risco nas Organizações, sejam quais forem os objetivos dos seus negócios, devem ser orientados à Segurança da Informação, pois a simples exposição de Informação confidencial, ou a perda de Informação, ou a ausência de credibilidade da Informação, de determinada Organização, pode ter consequências judiciais relevantes, contraordenações consideráveis, perda de credibilidade, e até mesmo á extinção da Organização!

"*Hence the saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."* **Sun Tzu on the Art of War, III Atack by Stratagem sec. V a.C. [9]**

REFERÊNCIAS BIBLIOGRÁFICAS

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2013). NP ISO 27001:2013 - Tecnologia de informação Técnicas de segurança Sistemas de gestão de segurança da informação – Requisitos.

[2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2013). NP ISO 27002:2013 - Tecnologia de informação Técnicas de segurança – Código de boas praticas para Controlos de Segurança da informação.

[3] ISO/IEC 20000-1: 2011 - Information technology - Service management - Part 1: Service management systems requirements

[4] ISO/IEC 20000-2: 2012 - Information technology - Service management - Part 2: Guidance on application of service management systems.

[5] ISO/IEC 31000:2009 - Risk Management - Principles and guidelines

[6] Diretiva UE 2016/1148 do Parlamento Europeu e do Conselho. Jornal Oficial Da União Europeia.

[7] (a) Republica, D. da. (2012). Resolução do Conselho de Ministros N. 91 de 2012 (RNID). Diário Da Repúbilica, 1.a Série - N. 216 - 8 de Novembro de 2012. (b) Republica, D. da. (2018). Resolução do Conselho de Ministros N. 2 de 2018 (RNID). Diário Da Repúbilica, 1.a Série - N. 4 - 5 de Janeiro de 2018.

[8] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Jornal Oficial Da União Europeia.

[9] Giles, L. (2000). Sun Tzu on the Art of War. (C. E. Series, Ed.). England: Allandale Online.