DGSI01

POLÍTICA DE SEGURANÇA

CYPE Ingenieros

EDIÇÃO	00
ALTERAÇÃO	Edição inicial
DATA	17/12/2024
ELABORADO	Responsável pela Segurança
REVISTO E APROVADO	Direção geral

ÍNDICE

1. DECLARAÇÃO DE PRINCÍPIOS

A CYPE INGENIEROS S.A., doravante a EMPRESA, é uma empresa com mais de 40 anos de experiência na comercialização, distribuição e pós-venda de software técnico para profissionais de Arquitetura, Engenharia e Construção. A EMPRESA oferece uma variedade de programas inovadores que foram concebidos para ajudar os profissionais na realização de cálculos estruturais, na gestão de projetos e no controlo de qualidade de maneira eficiente e precisa, tanto a nível nacional como internacional.

Devido à nossa atividade, na EMPRESA estamos conscientes de que a informação é um ativo de alto valor para a nossa organização e, portanto, requer uma proteção e gestão adequadas com o fim de dar continuidade à nossa linha de negócio e minimizar os possíveis danos ocasionados por falhas à integridade, disponibilidade e confidencialidade da informação. Do mesmo modo, tanto a legislação vigente relativa à proteção de dados pessoais (RGPD e LOPDGDD) como o compromisso da EMPRESA com os nossos clientes, fazem com que estejamos especialmente sensibilizados para o tratamento dos dados pessoais a que temos acesso no exercício da nossa atividade.

Para isso, a EMPRESA estabelece um conjunto de atividades de gestão que têm como objetivo preservar os princípios de confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e conformidade regulamentar da informação. Por sua vez, estes princípios são definidos da seguinte forma:

- **Confidencialidade**: é a propriedade que permite garantir que o acesso à informação só pode ser exercido pelas pessoas autorizadas a fazê-lo.
- **Integridade**: é a propriedade de salvaguardar a exatidão e a completude dos ativos de informação.
- **Disponibilidade**: é a qualidade que garante que as pessoas autorizadas podem aceder à informação e processá-la em qualquer momento em que seja necessária.
- **Autenticidade**: é a propriedade ou caraterística consistente em que uma entidade é quem diz ser, ou que garante a fonte dos dados.
- **Rastreabilidade**: é a propriedade ou caraterística consistente em que as ações de uma entidade podem ser imputadas exclusivamente a essa entidade.
- **Conformidade regulamentar**: é a propriedade que assegura que a informação é gerida de acordo com os princípios éticos, profissionais e legais estabelecidos pela regulamentação que se aplica em cada contexto.

Os sistemas devem ser protegidos contra ameaças em rápida evolução, com potencial para afetar a informação e os serviços. Para se defender destas ameaças, é necessária uma estratégia que se adapte às alterações das condições, para garantir a prestação contínua dos serviços.

Isto implica que os diferentes departamentos devem aplicar as medidas mínimas de segurança exigidas pelo Sistema Nacional de Segurança (ENS), bem como monitorizar continuamente os níveis de prestação de serviços, acompanhar e analisar as vulnerabilidades notificadas e preparar uma resposta efetiva a incidentes para garantir a continuidade dos serviços prestados.

Os diferentes departamentos da organização devem garantir que a segurança é uma parte integral de todas as fases do ciclo de vida do sistema, desde a sua conceção até à sua retirada de serviço, passando pelas decisões de desenvolvimento ou de aquisição e as atividades de funcionamento. Os requisitos de segurança e as necessidades de financiamento devem identificar-se e incluir-se no planeamento, nos pedidos de propostas e nos documentos de licitação para projetos TIC.

Os departamentos devem estar preparados para prevenir, detetar, reagir e recuperar de incidentes, em conformidade com o artigo 8º do ENS.

A proteção da privacidade está integrada no que precede. Os sistemas da EMPRESA tratam dados pessoais sensíveis e, por isso, a proteção da privacidade é um pilar essencial no quadro de um sistema de gestão da segurança da informação (SGSI) e constitui uma necessidade social que as empresas devem respeitar e proteger, bem como um objeto de legislação e/ou regulamentação específica em todo o mundo.

1.1. Objetivos gerais

A Política de Segurança proporciona as bases para definir e delimitar os objetivos e as responsabilidades pelas diversas ações técnicas, legais e organizativas necessárias para garantir a segurança da informação e a privacidade, em conformidade com o quadro legal aplicável e as políticas globais e específicas da EMPRESA, bem como os procedimentos definidos.

Estas ações, do ponto de vista da segurança e da privacidade, são selecionadas e implementadas com base numa análise de risco e no equilíbrio entre o risco aceitável e o custo das medidas.

O objetivo da Política de Segurança é fixar o quadro de ações necessárias para proteger os recursos de informação e dados contra ameaças, internas ou externas, deliberadas ou acidentais.

A informação e os dados podem existir numa variedade de formatos, com suportes tanto eletrónicos como em papel ou outros meios, e incluem, por vezes, dados críticos sobre as operações, estratégias ou atividades da EMPRESA e dos seus clientes, e inclusive, em certos casos, dados de caráter sensível conforme estabelece o regulamento de proteção de dados de caráter pessoal. A perda, corrupção ou roubo de informação ou dos sistemas que a gerem tem um impacto elevado na EMPRESA.

A EMPRESA está convencida de que uma gestão eficaz da segurança da informação e da privacidade é um elemento que permite à organização compreender completamente os riscos a que a informação está exposta e agir de forma adequada, bem como ser capaz de responder e adaptar-se de forma eficiente aos crescentes requisitos dos organismos reguladores, das leis e, naturalmente, dos seus clientes.

1.2. Compromisso da Direção

O propósito do sistema de gestão de segurança da informação é garantir que os riscos para a segurança da informação e a privacidade sejam conhecidos, assumidos, geridos e minimizados de forma documentada, sistemática, estruturada, repetível, responsável e adaptada às alterações que se produzem nos riscos, no ambiente e nas tecnologias.

Para isso, a Direção declara o compromisso da EMPRESA para:

- Estabelecer como objetivo principal o serviço de viagens ao estrangeiro com absoluto respeito pelos padrões de qualidade, preservando a informação, com especial atenção à sensibilidade dos dados pessoais tratados, com todas as medidas necessárias ao seu alcance.
- Aplicar o princípio da melhoria contínua a todos os processos da organização, com o objetivo adicional de alcançar o mais elevado grau de satisfação dos clientes.
- Assegurar o cumprimento dos requisitos legais e regulamentares aplicáveis (em particular os relacionados com a proteção de dados pessoais), bem como os que a organização tenha voluntariamente assumido.
- Promover a participação, a comunicação, a informação e a formação da equipa profissional com o objetivo de que se sinta envolvida no trabalho da organização como um todo.
- Promover o compromisso de responsabilização entre os membros da equipa, de acordo com os requisitos de qualidade, bem como os relativos à privacidade e segurança da informação acordados, tanto internamente como com os clientes, através de ações de formação e consciencialização adequadas e regulares.
- Assegurar a continuidade da atividade, desenvolvendo planos de continuidade de acordo com metodologias reconhecidas.
- Realizar e rever periodicamente uma análise de risco baseada em métodos reconhecidos que nos permitam estabelecer o nível tanto de privacidade dos dados pessoais, como de segurança da informação a nível geral, e dos projetos e serviços, em curso, e minimizar os riscos através do desenvolvimento de políticas específicas, soluções técnicas e acordos contratuais com organizações especializadas.
- Informar as partes interessadas.

- Seleção de fornecedores e subcontratados com base em critérios relacionados com a privacidade e a segurança da informação.

No que diz respeito especificamente à proteção dos dados pessoais, a EMPRESA compromete-se a cumprir os princípios estabelecidos na legislação aplicável. São eles:

- **Princípio de «licitude, lealdade e transparência»**. Os dados devem ser tratados de forma lícita, leal e transparente para o interessado.

- **Princípio de «finalidades»**. Os dados devem ser tratados para uma ou várias finalidades determinadas, explícitas e legítimas, e proíbe-se que os dados recolhidos com uns fins determinados, explícitos e legítimos sejam tratados posteriormente de forma incompatível com esses fins.

- **Princípio de «minimização dos dados»**. Aplicar medidas técnicas e organizativas para garantir que sejam objeto de tratamento os dados que unicamente sejam precisos para cada um dos fins específicos do tratamento, reduzindo a extensão do tratamento e limitando ao necessário o período de conservação e a sua acessibilidade.

- **Princípio de «exatidão»**. Dispor de medidas razoáveis para que os dados se encontrem atualizados, sejam eliminados ou se corrijam imediatamente quando sejam inexatos em relação aos fins para as quais são tratados.

- **Princípio de «limitação da conservação»**. A conservação dos dados deve limitar-se no tempo à realização dos fins a que se destina o tratamento.

- **Princípio de «segurança».** Realizar uma análise de risco orientada para a determinação das medidas técnicas e organizativas necessárias para garantir a integridade, a disponibilidade e a confidencialidade dos dados pessoais que se tratem.

- **Princípio de «responsabilidade ativa» ou «responsabilidade demonstrada»**. Manter a devida diligência de forma permanente para proteger e garantir os direitos e liberdades das pessoas singulares cujos dados são tratados com base numa análise dos riscos que o tratamento representa para esses direitos e liberdades, de modo a podermos garantir e demonstrar que o tratamento se ajusta às disposições do RGPD e a LOPDGDD.

- Dirigir, apoiar e supervisionar o sistema de gestão da segurança da informação, de acordo com o disposto no Decreto Real 311/2022 e alterações subsequentes, e garantir que os seus objetivos são alcançados.

A Direção da EMPRESA compromete-se a apoiar e promover os princípios estabelecidos nesta Política, solicitando aos colaboradores da empresa que assumam e cumpram as disposições do sistema de gestão documentado para o ENS.

1.3. Desenvolvimento da Política de Segurança

Esta Política de Segurança complementa as políticas de segurança da EMPRESA em diferentes matérias e será desenvolvida por meio de regulamento de segurança que aborda aspetos específicos. O regulamento de segurança estará à disposição de todos os membros da organização que necessitem de o conhecer e, em particular, daqueles que utilizam, operam ou administram os sistemas de informação e comunicações.

A documentação relativa à segurança da informação será classificada em três níveis, sendo que cada documento de um nível se fundamenta nos documentos de nível superior:

- **Primeiro nível**: Política de segurança.
- **Segundo nível**: Regulamentos e procedimentos de segurança.
- **Terceiro nível**: Relatórios, registos e evidências eletrónicas.

2. POLÍTICA

2.1. Prevenção

Os serviços devem evitar, ou pelo menos impedir tanto quanto possível, que a informação ou serviços sejam prejudicados por incidentes de segurança. Para o efeito, os departamentos devem implementar medidas mínimas de segurança determinadas pelo ENS, bem como qualquer controlo adicional identificado através de uma avaliação de ameaças e riscos. Estes controlos, bem como as funções e responsabilidades de segurança de todo o pessoal, devem estar claramente definidos e documentados.

Para garantir o cumprimento desta política, os departamentos devem:

- Autorizar os sistemas antes de os colocar em funcionamento.
- Avaliar regularmente a segurança, incluindo avaliações das alterações de configuração efetuadas por rotina.
- Solicitar a revisão periódica por terceiros, a fim de obter uma avaliação independente.

2.2. Deteção

Dado que os serviços podem degradar-se rapidamente devido a incidentes, que vão desde um simples abrandamento até à paralisação, os serviços devem monitorizar a operação de forma contínua para detetar anomalias nos níveis de prestação de serviços e atuar em conformidade, segundo o estabelecido no artigo 9º do ENS.

A monitorização é particularmente relevante quando se estabelecem linhas de defesa de acordo com o artigo 8º do ENS. Devem ser estabelecidos mecanismos de deteção, análise

e notificação que cheguem aos responsáveis regularmente e quando se verifique um desvio significativo dos parâmetros que se tenham pré-estabelecido como normais.

2.3. Resposta

Os serviços devem:

- Estabelecer mecanismos para responder eficazmente a incidentes de segurança.
- Designar um ponto de contacto para as comunicações relativas a incidentes detetados noutros departamentos ou noutros organismos.
- Estabelecer protocolos para a troca de informação relacionada com o incidente. Isto inclui comunicações bidirecionais com as equipas de resposta a emergências informáticas (CERT, acrónimo em inglês).

2.4. Recuperação

Para garantir a disponibilidade dos serviços críticos, os departamentos devem desenvolver planos de continuidade dos sistemas como parte do seu plano geral de continuidade de negócio e atividades de recuperação.

2.5. Organização da segurança

Esta política aplica-se a todos os sistemas da EMPRESA e a todos os membros da organização, sem exceção.

A EMPRESA compromete-se a prestar os seus serviços de forma estruturada e em conformidade com os requisitos estabelecidos no seu sistema integrado de gestão, de modo a garantir um serviço ininterrupto conforme os requisitos de disponibilidade, segurança e qualidade para os clientes.

Devido à nossa atividade, na EMPRESA sabemos que a informação é um ativo de elevado valor para a nossa organização, sobretudo a dos nossos clientes, pelo que requer uma proteção e gestão adequadas com o fim de dar continuidade à nossa linha de negócio e minimizar os possíveis danos causados por falhas na segurança da informação.

Para o efeito, a organização:

- Protegerá adequadamente a confidencialidade, a disponibilidade, a integridade, a autenticidade e a rastreabilidade dos seus ativos de informação através da introdução de um conjunto de controlos para gerir os riscos de segurança relevantes.

- Dará prioridade à proteção e salvaguarda dos clientes e dos dados dos clientes como uma prioridade de negócio.

- Estabelecerá, implementará, monitorizará, manterá e melhorará continuamente a sua gestão da segurança da informação como parte da sua abordagem mais ampla de gestão empresarial, e manterá a certificação acreditada de acordo com normas adequadas.
- Gerirá quaisquer violações de segurança da informação de maneira oportuna e responsável e investirá em estratégias adequadas de deteção, resposta e correção.
- A intervalos planeados, testará os seus controlos de segurança da informação e as suas respostas a cenários que possam causar uma ameaça às suas operações.
- Proporcionará os recursos adequados à organização para estabelecer, manter e melhorar o ambiente de segurança segundo as condições adequadas à evolução do cenário de risco.
- Investirá nas competências dos colaboradores para levarem a cabo as suas tarefas e proporcionará a capacitação e a consciência adequadas relevantes para a sua função e a informação a que têm acesso.
- Assegurará que os seus fornecedores e organizações associadas façam o mesmo e que estabeleçam e façam cumprir regulamentos de segurança a todos aqueles a quem é transmitida qualquer informação.

2.5.1. Comité de Segurança

Os membros do Comité de Segurança são designados numa ata constitutiva, com indicação da pessoa designada e do cargo a desempenhar.

O secretário do Comité de Segurança será o responsável pela segurança e terá como funções:

- Convocar as reuniões do Comité de Segurança.
- Preparar os temas a tratar nas reuniões do Comité, fornecendo informação atempada para a tomada de decisões.
- Elaborar a ata das reuniões.
- Executar de forma direta ou delegada as decisões do Comité.
- O Comité de Segurança informará o diretor geral.

O Comité de Segurança terá as seguintes funções:

- Atender às preocupações da Direção e dos diferentes departamentos.
- Informar regularmente a Direção sobre o estado da segurança da informação.
- Promover a melhoria contínua do sistema de gestão da segurança da informação.

- Elaborar a estratégia de evolução da organização no que respeita à segurança da informação.
- Coordenar os esforços das diferentes áreas em matéria de segurança da informação, para assegurar que os esforços são consistentes, alinhados com a estratégia decidida e para evitar redundâncias.
- Desenvolver e rever regularmente a Política de Segurança para que seja aprovada pela Direção.
- Aprovar o regulamento de segurança da informação.
- Coordenar todas as funções de segurança da organização.
- Assegurar o cumprimento da regulamentação legal e sectorial aplicável.
- Assegurar o alinhamento das atividades de segurança com os objetivos da organização.
- Coordenar os planos de continuidade das diferentes áreas, de modo a garantir uma ação contínua no caso de que devam ser ativados.
- Coordenar e aprovar, se for caso disso, as propostas de projetos recebidas dos diferentes âmbitos de segurança, encarregando-se de controlar e apresentar regularmente o progresso dos projetos e anunciar eventuais desvios.
- Receber as preocupações em matéria de segurança da Direção da entidade e transmiti-las aos responsáveis dos departamentos competentes, obtendo destes as respostas e soluções correspondentes que, uma vez coordenadas, devem ser comunicadas à Direção.
- Recolher relatórios regulares dos responsáveis pela segurança dos departamentos sobre o estado da segurança da organização e potenciais incidentes. Estes relatórios são consolidados e resumidos para serem comunicados à Direção da entidade.
- Coordenar e dar resposta às questões transmitidas através dos responsáveis de segurança departamentais.
- Definir, no âmbito da política de segurança da empresa, a atribuição de funções e os critérios para alcançar as garantias pertinentes em relação à separação de funções.
- Elaborar e aprovar requisitos de formação e qualificação de administradores, operadores e utilizadores do ponto de vista da segurança da informação.

- Monitorizar os principais riscos residuais assumidos pela organização e recomendar possíveis ações para os enfrentar.
- Monitorizar o desempenho dos processos de gestão de incidentes de segurança e recomendar possíveis ações para os resolver. Em particular, assegurar a coordenação das diferentes áreas de segurança na gestão de incidentes de segurança da informação.
- Promover a realização de auditorias periódicas que permitam verificar o cumprimento das obrigações do organismo em matéria de segurança.
- Aprovar planos de melhoria da segurança da informação da organização. Em particular, assegurar a coordenação de diferentes planos que possam ser levados a cabo em diferentes áreas.
- Priorizar as ações em matéria de segurança quando os recursos sejam limitados.
- Garantir que a segurança da informação seja tida em conta em todos os projetos, desde a especificação inicial até à implementação. Em particular, deverá garantir a criação e utilização de serviços horizontais que reduzam a duplicação e apoiem um funcionamento harmonioso de todos os sistemas TIC.
- Resolver conflitos de responsabilidade que possam aparecer entre diferentes responsáveis e/ou entre diferentes áreas da organização.

2.5.2. Funções e responsabilidades

A seguir, apresentam-se as funções dos responsáveis pela organização:

Responsável pela informação

As suas funções serão as seguintes

- Responsabilidade final pela utilização de determinada informação e, por conseguinte, pela sua proteção.
- Responsável final por qualquer erro ou negligência que conduza a um incidente de confidencialidade ou de integridade (em matéria de proteção de dados) e de disponibilidade (em matéria de segurança da informação).
- Estabelecer requisitos de informação em matéria de segurança.
- Determinar e aprovar os níveis de segurança da informação.

- Aprovar a categorização do sistema no que respeita à informação.
- Cumprir as funções que estão indicadas nos documentos no âmbito do ENS.

Responsável pelo serviço

As suas funções serão as seguintes

- Estabelecer os requisitos do serviço em matéria de segurança.
- Determinar os níveis de segurança dos serviços.
- Aprovar a categorização do sistema no que respeita aos serviços.
- Cumprir as funções que estão indicadas nos documentos no âmbito do ENS.

Responsável pela segurança

As suas funções serão as seguintes

- Manter a segurança da informação tratada e dos serviços prestados pelos sistemas de informação na sua área de responsabilidade, de acordo com a política de segurança da informação da organização.
- Promover a formação e a consciencialização em matéria de segurança da informação na sua área de responsabilidade.
- Aprovar a declaração de aplicabilidade.
- Canalizar e supervisionar tanto o cumprimento dos requisitos de segurança do serviço prestado ou da solução que fornece, como as comunicações relativas à segurança da informação e à gestão de incidentes no âmbito deste serviço (PoC).
- Cumprir as funções que estão indicadas nos documentos no âmbito do ENS.

O responsável pela segurança será o secretário do Comité de Segurança, com as funções indicadas na secção 2.5.1 da presente política.

Responsável pelo sistema

As suas funções serão as seguintes:

- Desenvolver, operar e manter o sistema de informação durante todo o seu ciclo de vida, incluindo as suas especificações, a sua instalação e a verificação do seu correto funcionamento.
- Definir a topologia e a gestão do sistema de informação, estabelecendo os critérios para a sua utilização e os serviços nele disponíveis.

- Assegurar que as medidas de segurança são corretamente integradas no quadro geral de segurança.
- Propor a suspensão do tratamento de determinada informação ou da prestação de determinado serviço, caso se verifiquem deficiências graves de segurança, suscetíveis de afetar o cumprimento dos requisitos estabelecidos.
- Cumprir as funções que estão indicadas nos documentos no âmbito do ENS.

Responsável pela privacidade

As suas funções serão as seguintes:

- Coordenar todos os aspetos relacionados com a adequação das ações da EMPRESA em matéria de proteção de dados de carácter pessoal.
- Coordenar, juntamente com o responsável pela segurança, o cumprimento do ENS no que respeita à proteção dos dados de carácter pessoal.

2.5.3. Procedimentos de designação

O responsável pela segurança será nomeado pelo Comité de Segurança. A nomeação será revista de 2 em 2 anos ou quando o lugar ficar vago.

Do mesmo modo, os restantes cargos indicados na secção anterior serão nomeados pelo Comité de Segurança, mediante ata da reunião.

2.5.4. Revisão da Política de Segurança

Será missão do Comité de Segurança a revisão anual da presente Política de Segurança e a proposta de revisão ou manutenção da mesma. Será aprovada pela Direção e divulgada de modo a que todas as partes afetadas tenham conhecimento dela.

2.6. Dados de carácter pessoal

A EMPRESA, no âmbito da prestação dos seus serviços, trata dados de carácter pessoal particularmente sensíveis.

A documentação relacionada, à qual só as pessoas autorizadas terão acesso, contém os registos da atividade de tratamento dos dados em causa e dos respetivos responsáveis pelo tratamento. Todos os sistemas de informação da EMPRESA devem cumprir os níveis de segurança exigidos pela regulamentação em função da natureza e da finalidade dos dados de carácter pessoal.

2.7. Gestão de riscos

Todos os sistemas sujeitos a esta política devem realizar uma análise de risco, avaliando as ameaças e os riscos a que estão expostos. Esta análise deve ser repetida:

- regularmente, pelo menos uma vez por ano;
- quando houver alteração da informação tratada;
- quando houver alteração dos serviços prestados;
- quando ocorre um incidente grave de segurança;
- quando se notifiquem vulnerabilidades graves.

A fim de harmonizar as análises de risco, o Comité de Segurança estabelecerá uma avaliação de referência para os diferentes tipos de informação tratada e os diferentes serviços prestados. O Comité de Segurança racionalizará a disponibilidade de recursos para atender às necessidades de segurança dos diferentes sistemas, promovendo investimentos de carácter horizontal.

2.8. Obrigações dos colaboradores

Todos os membros da EMPRESA são obrigados a conhecer e a cumprir a presente Política de Segurança e o Regulamento de Segurança, cabendo ao Comité de Segurança dispor os meios necessários para que a informação chegue aos afetados.

Todos os membros da EMPRESA assistirão a uma sessão de consciencialização sobre segurança da informação pelo menos uma vez por ano. Será criado um programa de consciencialização contínua para todos os membros da EMPRESA, em especial para os novos colaboradores.

As pessoas responsáveis pela utilização, operação ou administração de sistemas devem receber formação sobre a utilização segura dos sistemas, na medida do necessário para efetuarem o seu trabalho. A formação é obrigatória antes de assumirem uma responsabilidade, quer se trate da sua primeira afetação ou de uma alteração de funções ou de responsabilidades profissionais.

2.9. Terceiras partes

Quando a EMPRESA prestar serviços a outras organizações públicas ou privadas ou tratar informação de outras organizações públicas ou privadas, estas serão informadas da presente Política de Segurança, serão criados canais para informar e coordenar os respetivos Comités de Segurança e serão estabelecidos procedimentos para reagir a incidentes de segurança.

Quando a EMPRESA utiliza serviços de terceiros ou transfere informação para terceiros, estes serão informados da presente Política de Segurança e do Regulamento de Segurança que se aplica a esses serviços ou informação. Esta terceira parte estará sujeita às obrigações estabelecidas nesse regulamento e poderá desenvolver os seus próprios procedimentos operacionais para lhe dar cumprimento. Devem ser estabelecidos procedimentos específicos de notificação e resolução de incidentes. Deve ser assegurado que os colaboradores de terceiras partes estejam devidamente consciencializados em matéria de segurança, pelo menos ao nível definido na presente Política.

Sempre que qualquer aspeto da política não possa ser cumprido por uma terceira parte, tal como descrito nos parágrafos anteriores, será necessário um relatório do responsável pela segurança que exponha os riscos envolvidos e a forma de os resolver. Este relatório deverá ser aprovado pelos responsáveis pela informação e pelos serviços afetados antes de se avançar.

3. LEGISLAÇÃO APLICÁVEL

Seguidamente, apresentam-se as leis que se consideram aplicáveis ao SGSI, bem como a definição da área responsável pela avaliação do seu impacto na organização.

LEI / REGULAMENTAÇÃO	RESPONSABILIDADE
Lei (Espanha) 39/2015, de 1 de outubro, sobre o Procedimento Administrativo Comum para as Administrações Públicas.	Assessoria jurídica
Lei (Espanha) 40/2015, de 1 de outubro. Estabelece e regula as bases do regime jurídico das Administrações Públicas, os princípios do sistema de responsabilidade das Administrações Públicas e o poder de impor sanções, bem como a organização e o funcionamento da Administração Geral do Estado e do seu sector público institucional para o desenvolvimento das suas atividades.	Assessoria jurídica
Decreto Real (Espanha) 311/2022, de 3 de maio, que regulamenta o Esquema Nacional de Segurança.	Assessoria jurídica
Lei Orgânica (Espanha) 1/2015, de 30 de março, que altera a Lei Orgânica 10/1995, de 23 de novembro, do Código Penal.	Assessoria jurídica

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.	Assessoria jurídica
Lei Orgânica (Espanha) 3/2018, de 5 de dezembro, de Proteção de Dados Pessoais e garantia dos direitos digitais.	Assessoria jurídica
Lei (Espanha) 34/2002 de Serviços da Sociedade da Informação (LSSI).	Assessoria jurídica
Lei (Espanha) 22/11, de 11/11/1987, de Propriedade Intelectual.	Assessoria jurídica
Lei (Espanha) 17/2001, de 7 de dezembro, de Marcas.	Assessoria jurídica
Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.	Assessoria jurídica
Lei (Espanha) 6/2020, de 11 de novembro, reguladora de determinados aspetos dos serviços eletrónicos de confiança.	Assessoria jurídica