**Termo de Abertura**

**Serviços de Auditoria de Segurança**

**2022GPI-Grupo06**

**UNIVERSIDADE POLITÉCNICA DO INTERIOR (UPI)**

**22/03/2022**



Lista de Conteúdos

[Sumário Executivo 3](#_Toc99399752)

[Finalidade/Justificação do Projeto 3](#_Toc99399753)

[Necessidade/Caso de Negócio 3](#_Toc99399754)

[Objetivos de Negócio 3](#_Toc99399755)

[Descrição do Projeto](#_Toc99399756)

[Partes Interessadas](#_Toc99399757)

[Critérios de Sucesso e Objetivos Mensuráveis do Projeto 4](#_Toc99399758)

[Requisitos e Pressupostos 4](#_Toc99399759)

[Restrições 4](#_Toc99399760)

[Definição Preliminar do Âmbito 4](#_Toc99399761)

[Riscos 5](#_Toc99399762)

[Entregáveis do Projeto 5](#_Toc99399763)

[Calendário Resumido de Marcos 5](#_Toc99399764)

[Orçamento do projeto 5](#_Toc99399765)

[Gestor do Projeto](#_Toc99399766)

[Equipa do projeto 6](#_Toc99399767)

# Sumário Executivo

No setor de TI, engenheiros(as) e especialistas estão constantemente a tentar **prevenir uma violação de segurança** em sistemas. Qualquer situação desse tipo pode resultar na **perda de dados** e no **encerramento** de determinadas **operações**. Tendo isto em conta para uma entidade importante como a Universidade Politécnica do Interior (UPI), que agrega vários serviços, alunos e docentes, é muito importante estabelecer normas e procurar abranger **normas do RGPD** bem como **alcançar o maior nível de segurança possível.**

Com este projeto pretende-se realizar uma **análise e avaliação do nível segurança** dos sistemas de informação da Universidade Politécnica do Interior (UPI), garantindo a **conformidade** do seu **modelo de gestão**, e da sua infraestrutura tecnológica, de acordo com as melhores práticas.

Esta avaliação deverá permitir à UPI aferir o estado de **segurança dos sistemas de informação**, identificar as eventuais **fragilidades**, definir um **plano de ação corretiva**, ter apoio periódico proporcionando uma **melhoria contínua** e criar condições para que a UPI possa certificar-se, num curto prazo, na norma ISO/IEC 27001.

# Finalidade/Justificação do Projeto

## Necessidade/Caso de Negócio

Face à existência do Regulamento Geral de Proteção de Dados que, possui coimas bastante elevadas pelo não cumprimento do mesmo, a Universidade Politécnica do Interior sentiu a necessidade de realizar uma auditoria de segurança de informação de dados para verificar se tudo se encontra consoante o regulamento. O requisito imposto pela instituição é que, caso sejam identificadas vulnerabilidades no sistema, estas devem ser devidamente corrigidas.

Tendo isto em conta, podemos concluir que a UPI é a população alvo da realização deste projeto, uma vez que, a realização do mesmo é unicamente para benefício da instituição.

## Objetivos de Negócio

O objetivo deste negócio é identificar o estado atual da segurança de informação da plataforma tecnológica da UPI, de modo que possam ser corrigidas as vulnerabilidades identificadas, procurando assim obter a certificação na norma ISO/IEC 27001 evitando a aplicação de coimas muito elevadas por não cumprimento do regulamento.

Por isso, podemos afirmar que com a obtenção deste certificado a UPI beneficia bastante com o negócio, como por exemplo:

* Ganha uma maior reputação o que se refletirá num possível aumento de alunos a cada ano que, por sua vez resultará num aumento de ganhos anual devido a custos como propinas, entre outros.
* Evita gastos em coimas de não cumprimento do Regulamento Geral de Proteção de Dados que conta com um valor mínimo de 20 000€.

# Descrição do Projeto

## Partes Interessadas

* Universidade Politécnica do interior (UPI): Adjudicante, entidade que pretende que o projeto seja desenvolvido.
* Adjudicatário, entidade contratada pelo adjudicante.

## Critérios de Sucesso e Objetivos Mensuráveis do Projeto

A Universidade Politécnica do Interior através dos relatórios acerca da auditoria, bem como os planos de evolução deverá conseguir avaliar a taxa de sucesso do projeto.

Relativamente aos objetivos do projeto, no fim do projeto os objetivos são:

* Obter o conhecimento do estado de segurança da informação e plataformas tecnológicas de suporte.
* A instituição deve-se encontrar em conformidade com as normas de segurança e o enquadramento no sistema de gestão da qualidade da UPI.
* Os colaboradores da UPI devem estar sensibilizados para os requisitos obrigatórios das normas de segurança.

## Requisitos e Pressupostos

A empresa selecionada para a realização do processo de auditoria de segurança de informação tem de possuir obrigatoriamente**:**

* Certificação da entidade auditora junto do Gabinete Nacional de Segurança de Portugal (GNS) como entidade credenciada para o efeito;
* Certificação internacional de Lead Auditor & Lead Implementer ISO/IEC 27001, Lead Auditor & Lead Implementer BS 25999 junto da BSI;
* Apresentação de referências efetivas nesta área de atuação, com acreditações e/ou credenciais que comprovem o know-how e experiência na vertente de segurança de informação;
* As certificações CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager) e ITIL (Information Technology Infrastructure Library), e a envolvência em grupos e fóruns internacionais na área de segurança de informação como entidade acreditada para o efeito deverão ser consideradas como uma mais-valia operacional para o processo de decisão.

## Restrições

* O prazo de conclusão das fases é de 90 dias (30 dias para a primeira fase e 60 dias para a segunda e terceira fase);
* O custo pela prestação dos serviços não pode exceder o montante global de €74.999,00 (setenta e quatro mil novecentos e noventa e nove euros), acrescido de IVA à taxa legal em vigor.

## Definição Preliminar do Âmbito

No projeto estão incluídas as seguintes ações:

* Diagnóstico/Auditoria global de segurança interna e externa;
* Análise e avaliação detalhada de vulnerabilidades e riscos de segurança com base nos requisitos das normas;
* Especificação de um plano de ação com medidas de correção e melhorias concretas com base em prioridade e criticidade.

Para dar o projeto como concluído, é necessário que o adjudicante (UPI) obtenha a Certificação ISO/IEC 27001/27002.

# Riscos

* Falta ou indisponibilidade de recursos;
* Perda de um elemento da equipa (pelos diversos motivos como adoecimento, desistência, etc.);
* Perda do projeto;
* Quebra do dever de sigilo por parte de um dos membros;
* Atraso na entrega dos componentes a ser analisados.

# Entregáveis do Projeto

* **Fase 1 - Diagnóstico de Segurança Aplicacional, Tecnológica e Legal;**
  + Output - Relatório confidencial relativo ao diagnóstico acima referido, em formato digital editável e, sempre que aplicável, suscetível de posterior tratamento automático (base de dados);
* **Fase 2 - Auditoria transversal de Segurança de Informação (norma ISO/IEC 27001);**
  + Output - Relatório confidencial relativo ao diagnóstico acima referido, em formato digital editável e, sempre que aplicável, suscetível de posterior tratamento automático (base de dados);
* **Fase 3 - Preparação da UPI para a certificação ISO/IEC 27001/27002.**
  + Output - Plano de evolução da UPI para a melhoria do seu nível de segurança e otimização dos recursos inerentes aos sistemas de informação em vigor na UPI.

# Calendário Resumido de Marcos

* Fase 1 - Diagnóstico de Segurança Aplicacional, Tecnológica e Legal
* Fase 2 - Auditoria Transversal de Segurança de Informação (norma ISO/IEC 27001)
* Fase 3 - Preparação da UPI para a Certificação ISO/IEC 27001/27002

Os serviços inerentes à Fase 1 devem estar concluídos no prazo de 30 dias, já os serviços inerentes à Fase 2 e 3 devem estar concluídos no prazo de 60 dias.

# Orçamento do projeto

O orçamento máximo fornecido pela Universidade Politécnica do Interior, pela prestação dos serviços objeto, bem como pelo cumprimento das diversas obrigações apresentadas, não deve exceder o montante global de 74 999€, acrescido de IVA à taxa global legal em vigor.

Este orçamento inclui custos, encargos e despesas das quais não se encontram expressamente atribuídas à UPI, incluindo as despesas de aquisição, transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

# Gestor do Projeto

O gestor deste projeto é o Bruno Ferreira e deverá ser responsável por:

* Prever e gerir os principais problemas identificados no projeto.
* Gerir os stakeholders
* Divulgar de forma clara e objetiva todas as informações referentes ao projeto
* Gerir a equipa e as suas devidas tarefas
* Planeamento do consumo de recursos, bem como o seu devido acompanhamento e gestão ao longo do projeto.
* Pôr em prática as áreas de conhecimento do PMBOK
* Assegurar que o projeto será entregue com qualidade e excelência.

# Equipa do projeto

* **Sponsor** - É um dos principais defensores do projeto e é responsável por criar um alinhamento dos objetivos do projeto com a estratégia da empresa. Deve facilitar a resolução de problemas relacionadas com o projeto aprovar ou não mudanças, aprovar ou não o fato de assumir ou ignorar alguns riscos e ajudar na decisão por objetivos conflitantes.
* **Gestor do Projeto** - Gere e conduz todas as partes interessadas de modo a alcançar os objetivos do projeto.
* **Equipa de Gestão do Projeto** - Membros da equipa do projeto diretamente envolvidos nas atividades de gestão e liderança do projeto.