**Âmbito do Projeto**

**Serviços de Auditoria de Segurança**

**2022GPI-Grupo06**

**UNIVERSIDADE POLITÉCNICA DO INTERIOR (UPI)**

**04/04/2022**



Lista de Conteúdos

[Objetivos do projeto 3](#_Toc100006655)

[Descrição do âmbito do(s) produto(s) 3](#_Toc100006656)

[Requisitos do Projeto 3](#_Toc100006657)

[Necessidades e expectativas dos stakeholders 4](#_Toc100006658)

[Limites do projeto 4](#_Toc100006659)

[Entregáveis do projeto 4](#_Toc100006660)

[Critérios de aceitação 4](#_Toc100006661)

[Pressupostos detalhados do projeto 5](#_Toc100006662)

[Restrições do projeto 5](#_Toc100006663)

[Organização inicial do projeto 6](#_Toc100006664)

[Definição inicial dos riscos 6](#_Toc100006665)

[Marcos mais importantes e datas impostas 6](#_Toc100006666)

[Limitações relativamente a fundos 7](#_Toc100006667)

[Estimativa de custos 7](#_Toc100006668)

[Requisitos associados ao Sistema de Gestão de Qualidade 7](#_Toc100006669)

[Especificações do projeto 7](#_Toc100006670)

# Objetivos do projeto

Devido à existência do Regulamento Geral de Proteção de Dados que aplica coimas bastante elevadas pelo não cumprimento das regras que, podem ir até um máximo de 20 milhões de euros, a UPI sentiu a necessidade de realizar uma **análise e avaliação do nível de segurança** dos sistemas de informação, de modo a garantir a conformidade do seu modelo de gestão e da sua infraestrutura tecnológica, de acordo com as melhores práticas da atualidade. Deste modo, evita serem cometidas infrações e, consequentemente, despender de uma grande quantia de dinheiro que decerto causaria um grande dano financeiro à instituição.

Além do facto de evitar coimas de um valor exorbitante, a UPI ganha uma maior reputação pelo seu alto nível de segurança do sistema de informação que, por sua vez se pode refletir num aumento de alunos anual que, consequentemente resulta num aumento de ganhos anual devido aos custos que cada aluno acarreta, como por exemplo as propinas.

A UPI pretende ter o projeto concluído com qualidade ao fim de 90 dias após o seu início para que, dada ao aumento de qualidade das suas infraestruturas tecnológicas, certificar-se consoante a norma ISO/IEC 27001.

# Descrição do âmbito do(s) produto(s)

Para este projeto devem ser realizadas 3 entregas periódicas, uma entrega por fase, que, no fim das suas realizações terão um respetivo output, tal como se pode ser observado de seguida:

* Um relatório confidencial relativo ao Diagnóstico de Segurança Aplicacional, Tecnológica e Legal
* Um relatório confidencial relativo à Auditoria transversal de Segurança de Informação
* A elaboração de um plano de evolução de modo a preparar a UPI para a certificação ISO/IEC 27001/27002

Para cada relatório sempre que aplicável, deve ser suscetível de posterior tratamento automático (base de dados).

# Requisitos do Projeto

1. As ações a implementar na execução deste contrato deverão ter em conta as normas ITIL, ISO/IEC 27001/27002 e BS25999, de forma a:
   * Identificar claramente o estado atual da segurança de informação da plataforma tecnológica da UPI;
   * Corrigir as vulnerabilidades e riscos diagnosticados;
   * Apoiar a definição de procedimentos de segurança transversais e eficientes na gestão das aplicações e tecnologias de SI;
   * Garantir um plano de contingência eficiente.
2. Assim sendo, a prestação de serviços deverá contemplar, pelo menos, 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;

# Necessidades e expectativas dos stakeholders

* A UPI necessita de melhorar a segurança do seu sistema de informação para garantir a conformidade do seu modelo de gestão e da sua infraestrutura tecnológico, sendo expectável que após esta melhoria não sejam aplicadas coimas pelo não cumprimento do **RGPD**.
* Dada a necessidade da realização de uma auditoria realizada pelo adjudicatário, a UPI necessita de fornecer acesso à sua rede.
* É expectável que, com a realização deste projeto, a UPI terá uma melhoria significativa referente à segurança do seu sistema de informação.
* Além da melhoria de segurança, é expectável que a UPI ganhe um nível de reputação maior visto que será uma instituição com segurança de qualidade e que, consequentemente, deve trazer à instituição um maior número de inscrições anuais.

# Limites do projeto

Dentro do projeto está incluído:

1. Diagnóstico/auditoria global de segurança interna e externa;
2. Análise e avaliação detalhada de vulnerabilidades e riscos de segurança com base nos requisitos das normas ITIL, ISO/IEC 27001/27002 e BS25999;
3. Especificação de um plano de ação com medidas de correção e melhorias concretas com base em prioridade e criticidade;
4. Preparação da UPI para a Certificação ISO/IEC 27001/27002.

Não está incluído no projeto o que não se encontra referido acima.

# 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.

# Critérios de aceitação

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.

Os objetivos para a conclusão do projeto 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.

# Pressupostos detalhados do projeto

Para a realização deste projeto, existe um conjunto de requisitos que a Universidade Politécnica do Interior pressupõe que o adjudicatário cumprirá, sendo eles:

* 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.

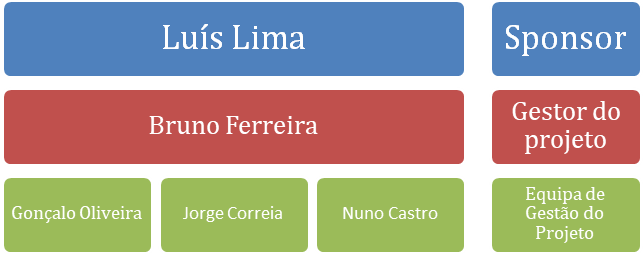
Dada a importância e grandeza de uma instituição como a Universidade Politécnica do Interior e a elevada importância e complexidade do projeto, o facto do adjudicatário possuir este conjunto de certificações, assegura que o mesmo é capaz de realizar o projeto com qualidade.

# Restrições do projeto

* O prazo de conclusão das fases é de 31/07/2022 (90 dias);
* 1ª Fase tem de ser finalizada até 31/05/2022 (30 dias);
* 2ª e 3ª Fase tem de ser finalizada até 31/07/2022 (60 dias);
* 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.
* Deve ser guardado sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à UPI. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros

# Organização inicial do projeto

Em baixo pode ser observado o organograma do projeto:



Ao longo deste projeto, estas serão as funções que cada cargo terá:

* **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.

# Definição inicial dos riscos

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

# Marcos mais importantes e datas impostas

* 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

A Fase 1 deve estar comprida até **31/05/2022.**

As Fases 2 e 3 devem estar compridas até **31/07/2022.**

# Limitações relativamente a fundos

A Universidade Politécnica do Interior definiu um limite de 74 999€ relativamente a fundos monetários.

Com a conclusão da Fase 1 deve ser realizado um pagamento de 50% do valor total

Com a conclusão da Fases 2 e 3 deve ser realizado um pagamento dos restantes 50% do valor total

# Estimativa de custos

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.

# Requisitos associados ao Sistema de Gestão de Qualidade

Para assegurar que possui qualificações suficientes para a realização do projeto, o adjudicatário deve possuir um conjunto de certificações que comprovem essas mesmas qualificações, tais como:

* 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.

O adjudicatário deve entregar um relatório de evolução do projeto no fim da última fase de modo que a UPI seja capaz de analisar o sucesso/evolução da melhoria de segurança do sistema de informação.

A execução dos serviços deverá respeitar as normas existentes, nomeadamente as normas ITIL – Information Technology Infrastructure Library, BS25999 e ISO/IEC 27001 e 27002.

# Especificações do projeto

* Os serviços executados neste projeto devem estar de acordo com as normas existentes, nomeadamente ITIL( Information Technology Infrastructure Library) , BS25999 e ISO/IEC 27001 e 27002.
* O adjudicatário deve entregar, no final da primeira e segunda fase, um relatório referente à fase e, na terceira e última fase deve ser entregue um plano de evolução da UPI para a melhoria do seu nível de segurança e otimização dos recursos inerentes aos sistemas de informação. Estes documentos permitirão à instituição analisar a evolução e verificar se os objetivos definidos foram alcançados com sucesso, permitindo à UPI aprovar as diferentes entregas.
* Como referido neste documento, a primeira fase terá uma duração de 30 dias que terá início no dia 1 de maio de 2022 e a segunda e terceira fase terão uma duração de 60 dias após o término da primeira fase. Será pago 50% do valor total do contrato na conclusão da primeira fase e, os restantes 50% serão pagos após a conclusão da fase 2 e 3. No entanto, caso sejam notificados atrasos nas entregas, a UPI tem o direito da retenção de até 10% do pagamento a efetuar.
* O adjudicatário deve possuir um conjunto de certificados que lhes permitam assegurar à UPI a qualidade do projeto que, já foram mencionados neste documento.