PLANO DE INTEGRIDADE E TRANSPARÊNCIA

INSTITUTO DE INFORMÁTICA
CONFIANÇA E INOVAÇÃO

ENTIDADE FORMADORA CERTIFICADA

EMPRESA CERTIFICADA eiC ISO 9001 Qualidade

EMPRESA CERTIFICADA eiC ISO/IEC 20000-1 Serviços de Tecnologias de Informação

EMPRESA CERTIFICADA eiC ISO/IEC 27001 Segurança da Informação

CONTROLO – HISTÓRICO DE ALTERAÇÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR	APROVAÇÃO
2016	v.1	Elaboração do Plano	Gestor do Plano	Conselho Diretivo
2018	v.2	Alteração do n.º 3 do artigo 9.º do Código de Ética e de Conduta Adição do n.º 4 e 5 do artigo 9.º do Código de Ética e de Conduta	Gestor do Plano	Conselho Diretivo
2018	v.3	Alteração do n.º 2 do artigo 1.º do Regulamento de Utilização de Informação Adição do n.º 8 do artigo 1.º do Regulamento de Utilização de Informação Adição de novo n.º 10 do artigo 3.º do Regulamento de Utilização de Informação Renumeração do n.º 10 do artigo 3.º para n.º 11 do Regulamento de Utilização de Informação Renumeração do n.º 11 do artigo 3.º para n.º 12 do Regulamento de Utilização de Informação Alteração do n.º 10 do artigo 3.º do Regulamento de Utilização de Informação Alteração do artigo 7.º do Regulamento de Utilização de Informação	Gestor do Plano	Conselho Diretivo
2021	v.4	Alteração do n.º 1 do artigo 6.º do Código de Ética e de Conduta Adição do n.º 2 do artigo 6.º do Código de Ética e de Conduta e subsequente renumeração do n.º 2 e 3 do referido artigo. Alteração de símbolos de certificação. Atualização das áreas orgânicas e respetivo organograma do Instituto.	Gestor do Plano	Conselho Diretivo
2022	v.5	Atualização das áreas orgânicas e respetivo organograma do Instituto (Deliberação (extrato) n.º 625/2022, de 25 de maio) Revisão do Plano de Integridade e Transparência, adequando ao DL 109-E/2021, de 9 de dezembro Atualização do Regulamento de Utilização de Tecnologias de Informação e Comunicação Revisão dos Riscos	Gestor do Plano	Conselho Diretivo
2024	v.6	Atualização das áreas orgânicas e respetivo organograma do Instituto Revisão do Plano de Integridade e Transparência adequando às recomendações do documento - PIT e os requisitos da Estrutura de Missão Recuperar Portugal v.1.2. e da OT n.º 14/2023 da EMRP. Aditamento do n.º 6 do art.º 9.º, n.º 2 do artigo 10.º e do artigo 15.º e 16.º, e alteração do n.º 1 do art.º 11.º, todos do Código de Ética e Conduta	Gestor do Plano	Conselho Diretivo

FICHA TÉCNICA
TÍTULO
PIT - PLANO DE INTEGRIDADE E TRANSPARÊNCIA

EDITOR
INSTITUTO DE INFORMÁTICA, I. P.
Av. Prof. Dr. Cavaco Silva, 17 – Edif. Ciência I – Tagus Park, 2740-120 Porto Salvo
Tel: 21 423 00 00

MISSÃO

Definir e propor as políticas e estratégias de tecnologias de informação e comunicação, garantindo o planeamento, conceção, execução e avaliação das iniciativas de informatização e atualização tecnológica do MTSSS.

VISÃO

Ser reconhecidos por transformar de forma inovadora e sustentável a relação do Cidadão com a administração pública, afirmando a diferenciação e a excelência dos nossos serviços.

VALORES

Inovação

Acreditamos na capacidade contínua de explorar novas ideias e soluções, que transformam a relação do cidadão com a administração pública.

Confiança

Cumprimos os nossos compromissos, assumimos riscos de forma responsável.

Competência

Valorizamos os contributos das pessoas, promovendo a comunicação e o trabalho em equipa. Juntos, conseguimos um trabalho de excelência.

Transparência

Somos eticamente responsáveis, acreditamos na prestação de contas e na boa gestão dos dinheiros públicos.

Os direitos de autor deste trabalho pertencem ao Instituto de Informática, I.P. (II, I.P.) e a informação nele contida encontra-se classificada em conformidade com a política de segurança da informação do II, I.P. (ver classificação atribuída no rodapé das páginas seguintes). Caso este documento não esteja classificado como "Público", não pode ser duplicado, destruído, arquivado, divulgado, ou transportado, na íntegra ou em parte, nem utilizado para outros fins que não aqueles para que foi fornecido, sem a autorização escrita prévia do II, I.P., em conformidade com o procedimento interno de manuseamento da informação do II, I.P., ou, se alguma parte do mesmo for fornecida por virtude de um contrato com terceiros, segundo autorização expressa de acordo com esse contrato. Todos os outros direitos e marcas são reconhecidos.

As cópias impressas não assinadas representam versões não controladas.

Índice

NOTA INTRODUTÓRIA 5
A. PLANO DE PREVENÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS 7
B. PLANO DE PREVENÇÃO DO RISCO DE FRAUDE 47
C. CÓDIGO DE ÉTICA E CONDUTA DO INSTITUTO 55
D. REGULAMENTO DE UTILIZAÇÃO DE INFORMAÇÃO 61
E. REGULAMENTO DE UTILIZAÇÃO DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO 65
F. CÓDIGO DE CONDUTA DE FORNECEDORES 75

NOTA INTRODUTÓRIA

O Plano de Integridade e Transparência estabelece um conjunto de princípios e de regras, tendo subjacente uma lógica de *compliance e accountability* - destinadas à prossecução da missão do Instituto de Informática, I.P.

Este Plano pretende também, no mesmo passo, potenciar o desempenho individual e o comportamento em equipa, elevar o clima de confiança e aperfeiçoar os relacionamentos internos e externos, contribuindo para o reforço dos valores legalmente consagrados e publicamente divulgados do Instituto de Informática, I.P.

O Plano de Integridade e Transparência integra os seguintes instrumentos:

- Plano de Prevenção de Riscos de Corrupção e Infrações Conexas;
- Plano de Prevenção do Risco de Fraude;
- Código de Ética e Conduta do Instituto;
- Regulamento de Utilização da Informação;
- Regulamento de Utilização de Tecnologias de Informação e Comunicação;
- Código de Conduta de Fornecedores.

O Plano de Prevenção de Riscos de Corrupção e Infrações Conexas visa garantir a proteção dos princípios de interesse geral, pelos quais o Instituto de Informática, I.P. pauta o desenvolvimento da sua atividade, tais como a prossecução do interesse público, da igualdade, da proporcionalidade, da transparência, da justiça, da imparcialidade, da boa-fé e da boa administração, tendo presentes as possíveis condutas e atitudes (por ação ou omissão) dos diversos agentes.
Neste sentido e face à Recomendação nº 1/2009, publicada no Diário da República, II Serie, nº 140, de 22 de julho do Conselho de Prevenção da Corrupção, pretende-se com a conceção do plano a identificação dos riscos que podem comprometer tais princípios, e a definição das iniciativas e ações a desenvolver no sentido de minimizar esses riscos.

Através do Plano de Prevenção do Risco de Fraude o Instituto de Informática, I.P., avalia o risco de fraude efetiva, combinada com um compromisso claro de combate à fraude, prevenindo potenciais infrações, uma vez que é crucial a gestão adequada e cuidadosa dos riscos associados à fraude. Todos os participantes na execução do Mecanismo de Recuperação e Resiliência (MRR) possuem a responsabilidade de demonstrar que tentativas de defraudar o orçamento da União Europeia (UE) não são aceitáveis e não serão toleradas.

Através do Código de Ética e de Conduta, o Instituto de Informática, I.P. estabelece normas que incluem práticas de ética e conformidade regulamentar. Com a adoção deste Código pretende-se a qualificação permanente dos trabalhadores, concretizada através de uma forte aposta não só na formação e valorização técnica do potencial humano, mas também na ética e na motivação, incentivando e promovendo o mérito, a competência, a participação e o empenho, reforçando uma cultura de exigência

e qualidade na prossecução do interesse público. Com o presente Código, dá-se cumprimento ao estipulado no art.º 7.º do Regime Geral de Prevenção da Corrupção (RGPC), anexo ao Decreto-Lei n.º 109-E/2021, de 9 de dezembro. Estas normas aplicam-se a todos os trabalhadores do Instituto de Informática, I.P., independentemente da natureza do vínculo ou posição hierárquica que ocupem.

O Regulamento de Utilização da Informação assume especial importância no Instituto – por ser uma entidade que gere bases de dados pessoais, e como tal sujeita ao regime jurídico prescrito pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, e às diferentes recomendações e orientações da Comissão de Proteção de Dados. Cada trabalhador ou colaborador externo que tenha acesso a dados pessoais (especialmente os sensíveis) passa a dispor - através da aprovação deste regulamento - de um instrumento regulador, no estrito cumprimento das obrigações de confidencialidade e de sigilo.

O Regulamento de Utilização das Tecnologias de Informação tem como objetivo estabelecer diretrizes e regular a utilização dos recursos tecnológicos, bem como atribuir responsabilidades e definir direitos e deveres dos utilizadores. Pretende igualmente gerir expetativas de acesso e utilização, no cumprimento das orientações da Comissão Nacional de Proteção de Dados, em especial, promovendo a segregação entre os conteúdos de caráter pessoal do trabalhador e os que são essenciais para o desenvolvimento das tarefas de interesse público que lhe estão cometidas, e cuja relevância ultrapassa a duração do vínculo.

O Código de Conduta de Fornecedores pretende que todos aqueles que estabelecem relações contratuais com o Instituto de Informática, I.P., no domínio, designadamente, da aquisição de bens e serviços, tenham um comportamento preventivo, no sentido do cumprimento de regras importantes no âmbito da legislação laboral, da proteção da igualdade e não discriminação, e do correto agir comercial. Embora estejamos perante um documento sem força coerciva, este código não deixa de estabelecer os padrões de exigência e integridade que o Instituto de Informática, I.P. espera dos seus fornecedores.

A adoção dos valores e princípios expressos neste Plano de Integridade e Transparência apresenta-se como um desígnio estratégico que deve ser seguido por todos.

Assim sendo, estabeleceu-se a obrigatoriedade da frequência de cursos anuais de *e-learning* que versem sobre os conteúdos deste Plano.

A implementação, execução e avaliação do Plano de Integridade e Transparência, será uma preocupação permanente de toda a organização, em particular dos seus dirigentes, mas será em primeira linha da responsabilidade do Responsável pela Conformidade Anticorrupção.

Importa por fim enfatizar que, por se tratar de um instrumento de enquadramento e apoio à ação, o seu conteúdo será periodicamente revisto e, sempre que necessário, atualizado.

A. PLANO DE PREVENÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS

1. ESTRUTURA ORGÂNICA DO INSTITUTO DE INFORMÁTICA, I.P.

1.1. Missão

A missão do Instituto de Informática, I.P., estipulada no n.º 1 do artigo 3.º do Decreto-Lei nº 196/2012, de 23 de agosto, é a seguinte:

O Instituto de Informática, I.P. tem por missão definir e propor as políticas e estratégias de tecnologias de informação e comunicação, garantindo o planeamento, conceção, execução e avaliação das iniciativas de informatização e atualização tecnológica do Ministério do Trabalho, Solidariedade e Segurança Social.

1.2. Atribuições

São atribuições do Instituto de Informática, I.P. nos termos do n.º 2 do artigo 3.º do Decreto-Lei nº 196/2012, de 23 de agosto:

a) Elaborar o plano estratégico de sistemas de informação;

b) Definir e controlar o cumprimento de normas e procedimentos relativos à seleção, aquisição e utilização de infraestruturas tecnológicas e sistemas de informação, enquanto organismo setorial do MSSS, para as áreas das tecnologias de informação e comunicação;

c) Assegurar a construção, gestão e operação de sistemas aplicacionais e de infraestruturas tecnológicas nas áreas de tecnologias de informação e comunicação dos serviços e organismos do MSSS, numa lógica de serviços comuns partilhados;

d) Promover a unificação e a racionalização de métodos, recursos, processos e infraestruturas tecnológicas nos serviços e organismos do MSSS, assegurando, designadamente, e nos termos fixados no plano estratégico previsto na alínea a), a aquisição, instalação e funcionamento dos equipamentos informáticos, bem como a sua substituição;

e) Assegurar a articulação com os organismos com atribuições interministeriais na área das tecnologias de informação e comunicação;

f) Prestar serviços a departamentos da solidariedade e segurança social, do trabalho e emprego, bem como a outros departamentos da Administração Pública, a empresas públicas ou a

entidades privadas, com base em adequados instrumentos contratuais que determinem, designadamente, os níveis de prestação e respetivas contrapartidas.

1.3. Competências dos Departamentos e Áreas Orgânicas

A organização interna dos serviços do Instituto de Informática, I.P., *cfr.* Portaria n.º 17/2024, de 25 de janeiro, é constituída pelas seguintes unidades orgânicas nucleares:

a) Departamento de Arquitetura e Desenvolvimento;
b) Departamento de Gestão de Aplicações;
c) Departamento de Análise e Gestão de Informação;
d) Departamento de Administração de Sistemas;
e) Departamento de Apoio ao Utilizador;
f) Departamento de Gestão de Serviços e Relações Externas;
g) Departamento de Organização e Gestão de Pessoas.

Por deliberação do Conselho Diretivo podem ser criadas, modificadas ou extintas unidades orgânicas flexíveis, designadas por áreas, integradas ou não em unidades orgânicas nucleares, cujo número não pode exceder, em cada momento, o limite máximo de 17.

São as seguintes as competências das unidades orgânicas nucleares e flexíveis do Instituto de Informática, I.P.:

a) **Departamento de Arquitetura e Desenvolvimento** - (artigo 4.º da Portaria n.º 17/2024, de 25 de janeiro l e Deliberação (extrato) n.º 625/2022, de 25 de maio.

Unidade Orgânica Nuclear	Competência	Subunidade Orgânica Flexível	Competências
DAD DEPARTAMENTO DE ARQUITETURA E DESENVOLVIMENTO	Definir, normalizar, planear e controlar a arquitetura de sistemas, a estratégia tecnológica, a acreditação de soluções aplicacionais e a visão tecnológica do planeamento estratégico de sistemas de informação, da gestão da qualidade, da segurança de informação, e da gestão de riscos.	**ADA** **Área de Desenvolvimento e Acreditação**	a) Assegurar a modelização das bases de dados; b) Gerir as diferentes disciplinas do ciclo de vida de desenvolvimento, nomeadamente, gestão de projeto, arquitetura, análise, experiência de utilizador, programação, testes e acreditação; c) Assegurar a gestão do ciclo de vida das soluções aplicacionais, em exploração, sob responsabilidade da ADA, de acordo com o calendário, especificações técnicas, resultados e custos acordados; d) Desenvolver e manter atualizados os planos dos projetos de desenvolvimento das soluções aplicacionais, sob
		AETA **Área de Estratégia Tecnológica e Arquitetura**	a) Colaborar na definição, revisão e implementação do plano estratégico de sistemas de informação, na sua vertente técnica e tecnológica, garantindo o seu alinhamento com a missão, objetivos e arquitetura de sistemas; b) Definir a arquitetura de sistemas de informação, em termos lógicos e físicos, garantindo o seu alinhamento com as boas práticas e as tendências tecnológicas, de acordo com as normas em vigor; c) Assegurar a coordenação técnica ao nível da segurança, monitorização e gestão de riscos aplicacionais; d) Colaborar na avaliação permanente do desempenho técnico das soluções e sistemas aplicacionais em produção; e) Definir e dinamizar a utilização das metodologias e ferramentas no âmbito do ciclo de vida do desenvolvimento; f) Apoiar o Departamento de Gestão de Clientes na identificação das necessidades dos clientes em termos de sistemas de informação e soluções aplicacionais; g) Antecipar as tendências de mercado, explorar o potencial de novas soluções tecnológicas e fomentar a transformação digital.

b) **Departamento de Gestão de Aplicações** - (artigo 5.º da Portaria n.º 17/2024, de 25 de janeiro e Deliberação (extrato) n.º 1761/2013, de 30 de abril publicado em DR a 30 de setembro de 2013)

Unidade Orgânica Nuclear	Competência	Subunidade Orgânica Flexível	Competências
DGA DEPARTAMENTO DE GESTÃO DE APLICAÇÕES	**Compete ao Departamento de Gestão de Aplicações (DGA) apoiar a definição da arquitetura, o desenvolvimento e a implementação das aplicações, assim como, gerir o seu ciclo de vida.**	AAE Área de Aplicações Estruturais	a) Fazer o levantamento, análise de requisitos e desenvolvimento de aplicações dos temas de negócio associados à identificação, qualificação, gestão de agregados e relações familiares, e remunerações, bem como aos canais informacionais e outros sistemas estruturais, de acordo com o calendário, especificações técnicas, resultados e custos acordados com o cliente; b) Assegurar a gestão do ciclo de vida das soluções aplicacionais, em exploração, sob responsabilidade da AAE, de acordo com o calendário, especificações técnicas, resultados e custos acordados com o cliente; c) Desenvolver e manter atualizados os planos dos projetos de desenvolvimento das soluções aplicacionais da responsabilidade da AAE.
		APS Área de Proteção Social	a) Fazer o levantamento, análise de requisitos e desenvolvimento de aplicações dos temas de negócio associados às prestações da segurança social, incluindo as de âmbito social, à ação social, combate à pobreza e promoção da inclusão social de acordo com o calendário, especificações técnicas, resultados e custos acordados com o cliente; b) Assegurar a gestão do ciclo de vida das soluções aplicacionais, em exploração, sob responsabilidade da APS, de acordo com o calendário, especificações técnicas, resultados e custos acordados com o cliente; c) Desenvolver e manter atualizados os planos dos projetos de desenvolvimento das soluções aplicacionais da responsabilidade da APS.
		ARC Área de Receita e Contas	a) Fazer o levantamento, análise de requisitos e desenvolvimento de aplicações dos temas de negócio associados à arrecadação de receita, pagamentos, gestão da dívida, contabilização e respetivo apuramento financeiro, e ainda a componente de coimas, ilícitos e fiscalização, de acordo com o calendário, especificações técnicas, resultados e custos acordados com o cliente; b) Assegurar a gestão do ciclo de vida das soluções aplicacionais, em exploração, sob responsabilidade da ARC, de acordo com o calendário, especificações técnicas, resultados e custos acordados com o cliente; c) Desenvolver e manter atualizados os planos dos projetos de desenvolvimento das soluções aplicacionais da responsabilidade da ARC.
		ASP Área de Sistemas de Pensões	a) Fazer o levantamento, análise de requisitos e desenvolvimento de aplicações dos temas de negócio associados à atribuição de pensões de velhice, invalidez e sobrevivência do regime da Segurança Social, bem como de subsídios conexos, de acordo com o calendário, especificações técnicas, resultados e custos acordados com o cliente; b) Assegurar a gestão do ciclo de vida das soluções aplicacionais, em exploração, sob responsabilidade da ASP, de acordo com o calendário, especificações técnicas, resultados e custos acordados com o cliente; c) Desenvolver e manter atualizados os planos dos projetos de desenvolvimento das soluções aplicacionais da responsabilidade da ASP.

c) **Departamento de Análise e Gestão de Informação** - (artigo 6.º da Portaria n.º 17/2024, de 25 de janeiro e Deliberação (extrato) n.º 1762/2013, de 30 de abril publicado em DR a 30 de setembro de 2013)

Unidade Orgânica Nuclear	Competência	Subunidade Orgânica Flexível	Competências
DAGI DEPARTAMENTO DE ANÁLISE E GESTÃO DE INFORMAÇÃO	O Departamento de Análise e Gestão de Informação tem por missão conceber, planear, executar e controlar os projetos de produção e recolha de dados com vista ao seu tratamento como informação estatística, e à sua utilização como indicadores de gestão.		a) Conceber, desenvolver e gerir sistemas de disponibilização de dados e informação a entidades competentes para a sua solicitação, respeitando as regras de proteção de dados e confidencialidade estatística; b) Gestão e desenvolvimento de Datamarts; c) Assegurar a manutenção da informação nos diferentes canais de disponibilização de dados: • SESS(Sistema de Estatísticas da Segurança Social); • Internet; • Intranet. a) Apoiar o Departamento de Gestão de Clientes na identificação das necessidades dos clientes, em termos de disponibilização de dados de apoio à gestão; b) Gerir os utilizadores e acessos ao Sistema de Dados (SESS -WEB); c) Gerir protocolos de informação com outros organismos da Administração Pública nos domínios da extração de dados, para a construção de indicadores.

d) **Departamento de Administração de Sistemas** - (artigo 7.º da Portaria n.º 17/2024, de 25 de janeiro, Deliberação (extrato) n.º 1759/2013, de 30 de abril publicado em DR a 30 de setembro de 2013) e Deliberação (extrato) n.º 83/2021, de 21 de dezembro publicado em DR a 22 de janeiro de 2021.

Unidade Orgânica Nuclear	Competência	Subunidade Orgânica Flexível	Competências
DAS DEPARTAMENTO DE ADMINISTRAÇÃO DE SISTEMAS	Compete ao Departamento de Administração de Sistemas gerir as infraestruturas de tecnologias de informação e comunicação e assegurar a administração de sistemas.	ASA Área de Suporte Aplicacional	a) Colaborar no desenvolvimento e implementação do plano de infraestruturas de tecnologias de informação e de comunicações de acordo com a arquitetura definida; b) Assegurar a administração e exploração dos sistemas aplicacionais em produção, das plataformas de integração, a operação de sistemas e de bases de dados, garantindo a sua adequação permanente às necessidades e níveis de serviço acordados; c) Administrar os portais de internet, intranet e aplicações dos serviços e organismos referidos na missão e atribuições estabelecidas; d) Apoiar o Departamento de Gestão de Clientes na identificação das necessidades dos clientes em termos de sistemas de informação e soluções aplicacionais.
		AI Área de Infraestrutura	a) Conceber, desenvolver e implementar o plano de infraestruturas de tecnologias de informação e de comunicações de acordo com a arquitetura definida; b) Assegurar a operacionalidade, exploração e monitorização das infraestruturas nas suas componentes de hardware e networking e outros sistemas no âmbito da sua atuação, otimizando a gestão do centro de processamento de dados; c) Assegurar a administração dos sistemas operativos e plataformas de virtualização, garantindo a sua adequação permanente às necessidades e níveis de serviço acordados; d) Assegurar a administração e exploração das soluções de armazenamento e salvaguarda de dados.
		AMESI Área de Monitorização e Segurança da Informação	a) Coordenar todas as matérias referentes à Segurança da Informação; b) Elaborar e propor e implementar o Plano Estratégico de Segurança de Informação; c) Elaborar e propor o modelo de governação da Segurança de Informação; d) Assegurar a articulação com a AQA, no âmbito do Sistema de Gestão da Segurança de Informação; e) Garantir a segurança dos dados, através da definição e gestão de políticas de acessos aos diversos sistemas de informação e respetivos controlos; f) Assegurar o relacionamento externo no âmbito da Segurança de Informação; g) Emitir pareceres técnicos no âmbito da Segurança de Informação; h) Garantir a articulação com a assessoria jurídica, no âmbito das questões jurídicas referentes a matérias de Segurança da Informação e proteção de dados pessoais; i) Garantir a articulação com o Encarregado de Proteção de Dados, no âmbito das suas competências próprias e no quadro da aplicação do RGPD e demais legislação aplicável, a pedidos de dados pessoais solicitados por entidades públicas; j) Gerir e garantir o correto funcionamento do Centro de Controlo de Operações (CCO), com a função de Monitorizar todos os Sistemas e Serviços Críticos do MTSSS; k) Implementar e gerir o Centro de Operações de Segurança, denominado SOC, com o objetivo de monitorizar, detetar, analisar e reportar todos os ciberincidentes, assim como coordenar a sua resposta e resolução para toda a infraestrutura de suporte aos diversos sistemas de informação do MTSSS.

e) **Departamento de Apoio ao Utilizador** - (artigo 8.º da Portaria n.º 17/2024, de 25 de janeiro e Deliberação (extrato) n.º 1763/2013, de 30 de abril publicado em DR a 30 de setembro de 2013)

Unidade Orgânica Nuclear	Competência	Subunidade Orgânica Flexível	Competências
DAU DEPARTAMENTO DE APOIO AO UTILIZADOR	Compete ao Departamento de Apoio ao Utilizador, desenvolver, gerir e manter os serviços de apoio ao utilizador final interno ou externo.	API Área Produtividade e Inovação	a) Conceber, implementar e manter todo o apoio necessário aos postos de trabalhos dos utilizadores finais, em particular a estação padrão, a telefonia e comunicações unificadas, e outras ferramentas de apoio ao utilizador final; b) Conceber, implementar e manter as ferramentas de produtividade e colaborativas consideradas necessárias de acordo com a arquitetura e utilização definidas; c) Apoiar o Departamento de Gestão de Clientes na identificação das necessidades dos clientes em termos de sistemas de informação e soluções aplicacionais; d) Avaliar necessidades, definir especificações técnicas e promover processos aquisitivos dos equipamentos e licenciamento de software necessários para o utilizador final nomeadamente em termos de Posto de Trabalho, Portáteis/Tablets, Equipamentos de Impressão e Multifuncionais, Telefones IP, etc. e) Identificar, conceber e implementar projetos de renovação tecnológica e de inovação com o apoio de equipas de projeto matriciais, constituídas por recursos das áreas do Departamento de Administração de Sistemas e da Área de Suporte ao Utilizador, ou de outros departamentos se necessário.
		ASU Área de Suporte ao Utilizador	a) Assegurar o suporte aos utilizadores internos e externos dos nossos clientes na utilização dos sistemas de informação, respetiva infraestrutura técnica e demais serviços disponibilizados pelo Instituto de Informática, I.P., garantindo o respeito pelos níveis de serviço contratualizados, nomeadamente: b) Garantir a coordenação do serviço de apoio central e local, e a aplicação do processo de gestão de incidentes e pedidos de serviço. c) Assegurar, igualmente, a gestão da base de dados de conhecimentos inerente ao apoio técnico. d) Assegurar uma primeira linha central de apoio que assegura o atendimento a todos os utilizadores dos nossos clientes, registando e tratando os incidentes e pedidos de serviço reportados através dos diferentes canais disponibilizados (telefone, email, Web), analisando, informando, resolvendo e/ou reencaminhando para diversas equipas técnicas. e) Proceder ao acompanhamento das solicitações e à monitorização dos níveis de serviços acordados com o cliente. f) Garantir o apoio de proximidade aos utilizadores dos nossos clientes nos seus locais de trabalho. Asseguram o suporte e resolução de incidentes e pedidos de serviço relacionados com postos de trabalho e com as diversas infraestruturas técnicas existentes nos locais, bem como operacionalizar projetos de âmbito nacional. g) Assegurar o funcionamento e manutenção de diversos equipamentos e soluções informáticas.

f) **Departamento de Gestão de Serviços e Relações Externas**- (artigo 9.º da Portaria n.º 17/2024, de 25 de janeiro e Deliberação n.º 16/CD/2023.

Unidade Orgânica Nuclear	Competência	Subunidade Orgânica Flexível	Competências
DGSRE DEPARTAMENTO DE GESTÃO DE SERVIÇOS E RELAÇÕES EXTERNAS	Compete ao Departamento de Gestão de Serviços e Relações Externas, assumir o papel de principal contacto e promover a imagem junto dos parceiros, compreender as suas necessidades e assegurar um correto planeamento interno para o cumprimento de prazos, custos e receitas das soluções que garantam os adequados níveis de prestação e respetivas contrapartidas.	AREC Área de Relações Externas e Comunicação	a) Estabelecer e desenvolver o relacionamento com as entidades parceiras, utilizadoras das soluções tecnológicas do Instituto, assegurando a atribuição de um Gestor de Conta; b) Estabelecer Planos individuais de acompanhamento das entidades parceiras, assegurando as suas necessidades e a convergência com as linhas estratégicas definidas pelo Instituto, para o ano em causa; c) Criar instrumentos de monitorização e avaliação da relação com as entidades parceiras; d) Determinar os canais de comunicação apropriadas a cada público-alvo (destinatários da ação), em articulação com as entidades parceiras; e) Gerir e acompanhar o processo da cadeia de valor do Instituto, nomeadamente no âmbito da gestão do relacionamento de parceiros; f) Assegurar o acompanhamento das relações externas no âmbito de projetos internacionais do Instituto, apoiando o Conselho Diretivo e a atividade dos restantes Departamentos nas áreas internacionais; g) Assegurar a gestão e comunicação externa de serviços dirigidos a cidadãos e empresas, em particular no âmbito da Plataforma de serviços e Interoperabilidade; h) Gerir e administrar soluções e aplicações da responsabilidade do Instituto, nomeadamente o envio massivo de emails e a gestão documental; i) Implementar e acompanhar o estabelecimento de protocolos, garantindo procedimentos padronizados e de acordo com as melhores práticas; j) Prestar apoio ao Conselho Diretivo, Departamentos e Áreas, nomeadamente através da conceção, coordenação e execução de campanhas e suportes de comunicação interna e institucional; k) Desenvolver a estratégia de comunicação, visando nomeadamente implementar a política de comunicação do Instituto, assegurar a gestão da imagem corporativa, garantir o desenvolvimento criativo, a conceção gráfica e a produção de suportes e peças de comunicação e imagem, garantir a publicação da revista IInova do Instituto e gerir e monitorizar a presença do Instituto nos media e redes sociais; l) Conceber e concretizar iniciativas de envolvimento organizacional que promovam a coesão, a cultura organizacional, a missão e os valores do Instituto;

Unidade Orgânica Nuclear	Competência	Subunidade Orgânica Flexível	Competências
DGSRE DEPARTAMENTO DE GESTÃO DE SERVIÇOS E RELAÇÕES EXTERNAS	Compete ao Departamento de Gestão de Serviços e Relações Externas, assumir o papel de principal contacto e promover a imagem junto dos parceiros, compreender as suas necessidades e assegurar um correto planeamento interno para o cumprimento de prazos, custos e receitas das soluções que garantam os adequados níveis de prestação e respetivas contrapartidas.	ASSO Área de Serviços e Sustentabilidade Organizacional	a) Gerir e administrar as aplicações de suporte à gestão, prestação e utilização dos serviços de formação; b) Planear as atividades de formação, no âmbito do desenvolvimento de competências, em particular quanto aos utilizadores das soluções do Instituto, de acordo com os projetos e necessidades diagnosticadas; c) Promover, organizar e produzir cursos de formação e-learning e formação presencial, assim como recursos pedagógicos de apoio à utilização dos sistemas de informação do Instituto; d) Avaliar as atividades formativas, recolhendo resultados que permitam perceber os objetivos traçados nas ações desenvolvidas; e) Desenvolver um plano estratégico de gestão da mudança e implementar as medidas e ações de gestão da mudança, em articulação com as equipas de projetos, para apoiar e mobilizar as entidades parceiras, assim como os utilizadores de serviços e soluções disponibilizados pelo Instituto. f) Gerir o catálogo de serviços do Instituto, assegurando a coerência e consistência dos serviços disponibilizados, bem como a sua atualização regular, divulgação e promoção; g) Monitorizar os acordos de níveis de serviço (SLA) e os acordos de níveis operacionais (OLA); h) Em articulação com o Departamento de Administração de Sistemas e Departamento de Apoio ao Utilizador, garantir a monitorização dos serviços e a sua implementação na ferramenta de gestão de serviços TI (ITSM), respetivamente; i) Gerir e acompanhar os processos da cadeia de valor, nomeadamente no âmbito da gestão de alterações, gestão da procura e gestão de catálogo e níveis de serviço; j) Desenvolver uma estratégia de sustentabilidade do Instituto, visando nomeadamente definir e implementar uma estratégia de sustentabilidade tecnológica no âmbito do Instituto, alinhando-a com os objetivos de negócio; k) Identificar oportunidades de melhoria em práticas de sustentabilidade, estabelecendo metas e métricas para avaliar o desempenho sustentável e em articulação com o Departamento de Organização e Gestão de Pessoas, desenvolver políticas e práticas de compras sustentáveis; Promover programas de responsabilidade social corporativas que demonstram o compromisso do Instituto com a comunidade e o meio ambiente; l) Desenvolver parcerias com organizações externas, ONGs e instituições académicas para avançar na agenda de sustentabilidade e inovação. m) Desenvolver parcerias com organizações externas, ONGs e instituições académicas para avançar na agenda de sustentabilidade e inovação.

g) **Departamento de Organização e Gestão de Pessoas** - (artigo 10.º da Portaria n.º 17/2024, de 25 de janeiro e Deliberação n.º 15/CD/2023, de 24 de novembro.

Unidade Orgânica Nuclear	Competência	Subunidade Orgânica Flexível	Competências
DOGP DEPARTAMENTO DE ORGANIZAÇÃO E GESTÃO DE PESSOAS	Assegurar e apoiar o funcionamento interno do Instituto de Informática, I.P., nomeadamente nas áreas da gestão de recursos humanos, da gestão administrativa, orçamental e financeira e da gestão de aquisições de bens e serviços e de contratos. Conceber, rever, avaliar e atualizar o plano de atividades e produzir os respetivos relatórios de atividades de gestão.	ACP Área de Contratação Pública	a) Organizar e coordenar, em articulação com as restantes unidades orgânicas, as ações necessárias à elaboração de estudos de previsão e planeamento das aquisições de bens e serviços para o II, I.P., com vista à elaboração do Plano Anual de Compras; b) Assegurar a realização de todos os procedimentos de aquisição de bens e serviços e de empreitadas do II, I.P. em articulação com as demais unidades orgânicas em razão das respetivas competências; c) Assegurar a participação nos procedimentos centralizados de aquisição de bens e serviços, contribuindo com a identificação das necessidades do II, I.P.; d) Propor e pugnar pela aplicação de metodologias e normas procedimentais a observar no âmbito da contratação pública; e) Monitorizar a execução dos contratos celebrados pelo II, I.P. em articulação com os respetivos gestores dos contratos e com Área Financeira e Administrativa; f) Organizar, manter atualizada e publicitar a informação a reportar a entidades externas no âmbito das competências da Área; g) Proceder à avaliação periódica dos fornecedores e diligenciar pela adoção das medidas adequadas em face dos resultados obtidos.

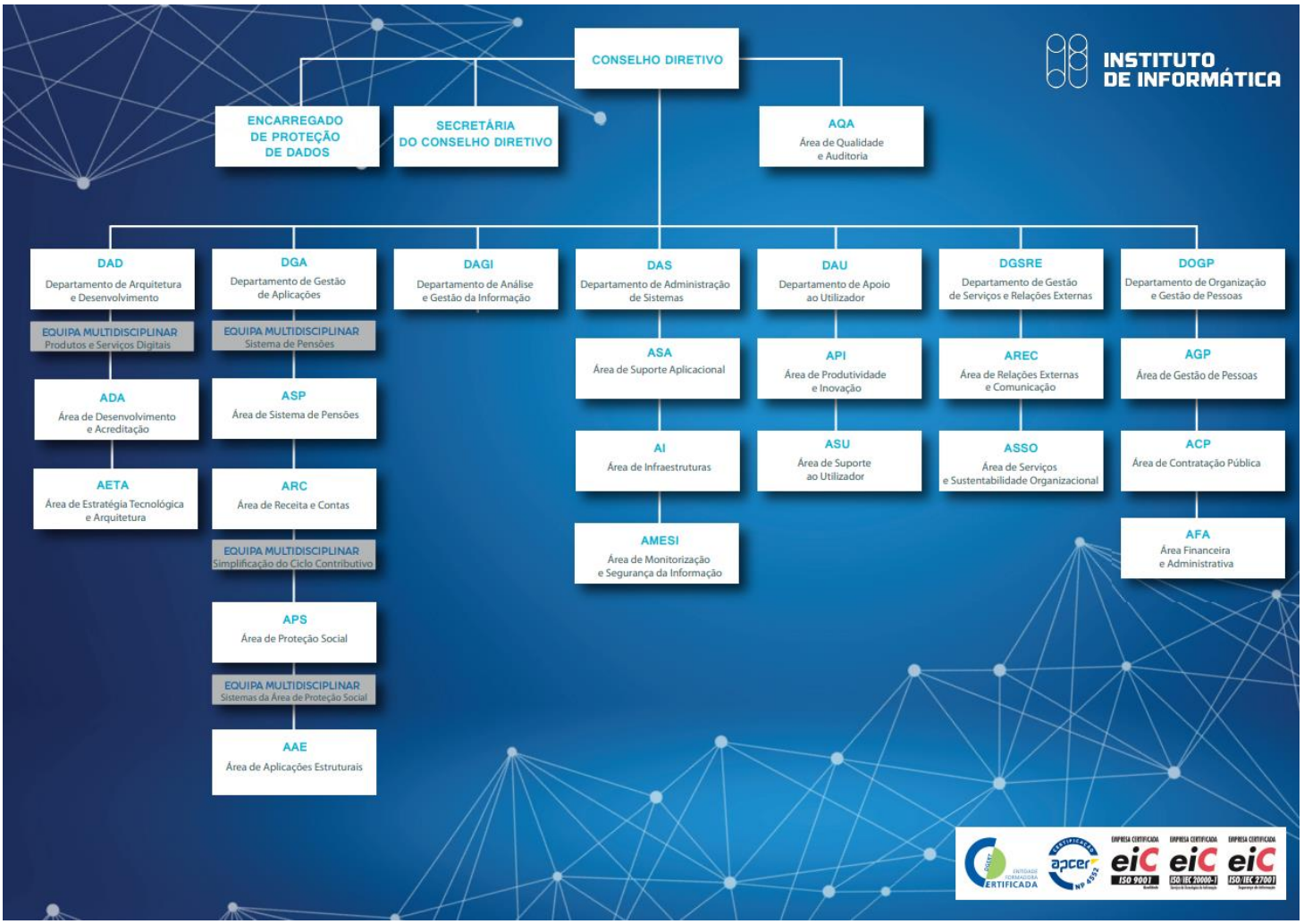
Unidade Orgânica Nuclear	Competência	Subunidade Orgânica Flexível	Competências
DOGP DEPARTAMENTO DE ORGANIZAÇÃO E GESTÃO DE PESSOAS	Assegurar e apoiar o funcionamento interno do Instituto de Informática, I.P., nomeadamente nas áreas da gestão de recursos humanos, da gestão administrativa, orçamental e financeira e da gestão de aquisições de bens e serviços e de contratos. Conceber, rever, avaliar e atualizar o plano de atividades e produzir os respetivos relatórios de atividades de gestão.	AFA Área Financeira e Administrativa	a) Assegurar a elaboração, o planeamento orçamental e controlo da sua execução; b) Assegurar a gestão financeira e patrimonial, produzindo e disponibilizando informação contabilística e financeira, para reporte aos Órgãos de Gestão, à Tutela, Tribunal de Contas, Instituto de Gestão Financeira da Segurança Social, I.P., Entidades Fiscalizadoras, bem como ao Fiscal Único do II, I.P; c) Assegurar a Contabilidade de Gestão, produzindo informação relevante e analítica sobre custos, rendimentos e resultados, como forma de apoio à gestão; d) Garantir o controlo e operações de tesouraria do II, I.P., gerindo os fluxos financeiros, com base no orçamento anual aprovado; e) Proceder à faturação dos serviços prestados e garantir o controlo e contabilização das receitas do II, I.P; f) Gerir os processos de candidatura a projetos cofinanciados e respetivo controlo e reporte de execução; g) Assegurar as prestações de contas mensais e anuais de acordo com as normas legais em vigor e elaborar relatórios periódicos de apoio à gestão; h) Coordenar as atividades administrativas e transversais ao funcionamento interno dos serviços, nomeadamente expediente e arquivo geral do II, I.P.; i) Gerir os contratos de aquisição de bens e serviços celebrados no âmbito do funcionamento interno do II, I.P.; j) Assegurar a gestão do edifício sede do II, I.P., garantindo as melhores condições de utilização e conforto das instalações; k) Gerir a frota automóvel do II, I.P., garantindo a disponibilidade de viaturas de serviço adequadas às necessidades dos serviços, bem como o reporte de informação à Entidade de Serviços Partilhados da Administração Pública, I.P.; l) Controlar os acessos ao edifício, garantindo o cumprimento das regras de identificação e circulação de pessoas; m) Assegurar a gestão do património, zelando pela conservação e utilização racional das instalações e garantir a atualização permanente do inventário; n) Assegurar o armazenamento de bens de utilização corrente, procedendo à gestão de stocks e reporte de necessidades de aquisição à Área de Contratação Pública.

Unidade Orgânica Nuclear	Competência	Subunidade Orgânica Flexível	Competências
DOGP DEPARTAMENTO DE ORGANIZAÇÃO E GESTÃO DE PESSOAS	Assegurar e apoiar o funcionamento interno do Instituto de Informática, I.P., nomeadamente nas áreas da gestão de recursos humanos, da gestão administrativa, orçamental e financeira e da gestão de aquisições de bens e serviços e de contratos. Conceber, rever, avaliar e atualizar o plano de atividades e produzir os respetivos relatórios de atividades de gestão.	AGP Área de Gestão de Pessoas	a) Concretizar, numa perspetiva de permanente desenvolvimento organizacional, auscultações internas e externas, elaborar estudos e pareceres com o objetivo de auditar as estruturas organizativas e respetivos postos de trabalho a fim de os adequar aos objetivos globais do II, I.P.; b) Assegurar a elaboração e a permanente atualização do plano de gestão previsional de gestão de pessoas, em função dos objetivos estratégicos e das prioridades superiormente definidos; c) Conceber, implementar e monitorizar indicadores de desempenho no âmbito da gestão de pessoas; d) Avaliar e desenvolver periodicamente as competências dos trabalhadores, em articulação com as necessidades estratégicas do II, I.P., e em consonância com as boas práticas e normas vigentes; e) Assegurar o processamento salarial e controlo de assiduidade e demais gestão administrativa, no cumprimento de princípios de equidade interna, das disposições normativas internas e da legislação em vigor; f) Promover medidas de conciliação da vida pessoal, profissional e familiar; g) Coordenar todas as atividades inerentes à saúde e segurança no trabalho, em consonância com a legislação em vigor, e concretizando outras iniciativas que promovam o bem-estar dos trabalhadores; h) Gerir e acompanhar os processos de recrutamento e seleção, bem como os processos de movimentação de pessoas do II, I.P., e assegurar o acolhimento e integração de novos trabalhadores; i) Promover a realização e acompanhamento dos processos de estágios curriculares e profissionais, com especial relevância para as áreas de tecnologias de informação e comunicação, em articulação direta com as necessidades estratégicas do II, I. P., j) Organizar, gerir, monitorizar e avaliar o plano de formação anual; k) Implementar, gerir e monitorizar o sistema de avaliação de desempenho individual, garantindo a operacionalização dos respetivos impactos.

h) **Área de Qualidade e Auditoria** - Deliberação n.º 806/2016, de 26 de abril, publicada na 2.ª série do Diário da República, de 10 de março de 2016 com a alteração da Deliberação n.º 12/CD/2023 de 16 de novembro.

Subunidade Orgânica Flexível	Competência	Outras Competências
AQA ÁREA DE QUALIDADE E AUDITORIA	Coordenar a implementação do modelo de planeamento estratégico e operacional, bem como assegurar a eficácia e a melhoria contínua do sistema de gestão integrado no âmbito do desenvolvimento e das políticas de melhoria contínua do Instituto de Informática, I.P..	a) Assegurar a coordenação do processo de planeamento estratégico de sistemas de informação do MSESS; b) Definir, implementar e controlar o sistema de Gestão e Avaliação de Desempenho Organizacional do Instituto de Informática, I.P.; c) Conceber, rever, avaliar e atualizar o plano de atividades e produzir os respetivos relatórios de atividades de gestão; d) Assegurar o apoio ao planeamento e gestão de projetos, acompanhar e controlar a sua execução; e) Planear, implementar, monitorizar, avaliar, rever e contribuir para melhorar continuamente o sistema de gestão integrado do Instituto de Informática, I.P. e a respetiva eficácia aos seguintes níveis: i. Sistema de gestão da qualidade; ii. Sistema de gestão de serviços de tecnologias de informação; iii. Sistema de gestão da continuidade do negócio; iv. Sistema da segurança da informação; v. Gestão do risco; vi. Sistemas de gestão da responsabilidade social; vii. Outras componentes e sistemas que venham a ser integrados no âmbito da estratégia do Instituto de Informática, I.P.. f) Coordenar as autoavaliações, assessment e auditorias ao sistema de gestão integrado e aos sistemas de informação operacionais, bem como as auditorias ao Sistema de Controlo Interno no âmbito do Plano de Recuperação e Resiliência.

1.4. Organograma



2. PLANO DE PREVENÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS

2.1. Enquadramento

O Conselho de Prevenção da Corrupção, doravante CPC, entidade administrativa independente que funciona junto do Tribunal de Contas, aprovou a Recomendação nº 1/2009, publicada no Diário da República, II Serie, nº 140, de 22 de julho, através da qual todos os organismos públicos são instados a elaborar Planos de Prevenção da Corrupção e Infrações Conexas, bem como relatórios anuais sobre a execução dos mesmos.

Esta recomendação surge na sequência de um questionário lançado a todos os organismos da administração pública, vertido na Deliberação do CPC, de 4 de março de 2009, com o objetivo de fazer uma avaliação da gestão dos riscos de corrupção nas áreas da contratação pública e da concessão de benefícios, ao qual o Instituto de Informática, I.P. respondeu.

A gestão do risco de corrupção assume um carácter transversal, sendo uma responsabilidade de todos os trabalhadores. São vários os fatores que podem influenciar situações de risco de corrupção e infrações conexas, destacando-se:

a) A competência da gestão;
b) A idoneidade dos gestores e decisores;
c) A qualidade do sistema de controlo interno e a sua eficácia;
d) A conduta dos trabalhadores das instituições e a existência de normas e/ou princípios que pautem a sua atuação;
e) A própria legislação, que por vezes não propicia, de forma fácil, a tomada de decisões sem riscos. Com efeito, a legislação a aplicar é muitas vezes burocratizante, complexa, vasta e desarticulada, impedindo uma gestão flexível e ágil dos recursos públicos que potencia o risco de existência de irregularidades.

Os planos de prevenção de riscos de corrupção são assim um instrumento de gestão fundamental que permitirá aferir a eventual responsabilidade que ocorra na gestão de recursos públicos.

Deste modo, a estrutura adotada para a elaboração do presente plano tem por base as orientações emanadas do guião disponibilizado no site do Conselho de Prevenção da Corrupção (www.cpc.tcontas.pt).

Mais recentemente, o CPC emitiu a 1 de abril de 2022 uma recomendação – "Boas Práticas de Cibersegurança", recomendando a todos os órgãos e entidades públicas, designadamente que:

- Promovam ações de formação e sensibilização em programas de Cibersegurança;
- Reúnam os meios técnicos adequados para garantir um elevado nível de Cibersegurança, dando cumprimento ao estabelecido no Decreto-Lei n.º 65/2021, de 30 de julho, e no regulamento n.º 183/2022, de 21 de fevereiro.

No âmbito da gestão e controlo do Plano de Recuperação e Resiliência (PRR), o Instituto de Informática, adotará as medidas adequadas para proteger os interesses financeiros da União e para assegurar que a utilização de fundos em relação a medidas apoiadas pelo PRR cumprem o direito da União e o direito nacional aplicáveis, em especial no que respeita à prevenção, deteção e correção de fraudes, corrupção, conflito de interesses e duplo financiamento.

2.2. Sobre o Plano

É intenção do Instituto de Informática, I.P. continuar a aperfeiçoar os seus processos, procedimentos e funções, apostando na transparência, na simplicidade, na monitorização e na responsabilidade.

Em 2022, o Instituto de Informática, I.P. procedeu à revisão do Plano de Prevenção de Riscos de Corrupção e Infrações Conexas ([1]), adaptando-o ao quadro normativo vigente, a Resolução do Conselho de Ministros n.º 37/2021, aprovada no dia 18 de março de 2021 e publicada em Diário da República no dia 6 de abril, onde foi aprovada a Estratégia Nacional Anticorrupção.

Aquele diploma, para além de reconhecer a necessidade de ajustar alguns aspetos do sistema repressivo, considera indispensável o fortalecimento e a valorização dos mecanismos de prevenção e deteção de crimes de corrupção e crimes conexos. A estratégia de combate à corrupção identifica sete prioridades para reduzir o fenómeno da corrupção em Portugal:

[1] Plano de Gestão de Riscos de Corrupção e Infrações Conexas 2021.

- Melhorar o conhecimento, a formação e as práticas institucionais em matéria de transparência e integridade;
- Prevenir e detetar os riscos de corrupção no setor público;
- Comprometer o setor privado na prevenção, deteção e repressão da corrupção;
- Reforçar a articulação entre instituições públicas e privadas;
- Garantir uma aplicação mais eficaz e uniforme dos mecanismos legais em matéria de repressão da corrupção, melhorar o tempo de resposta do sistema judicial e assegurar a adequação e efetividade da punição;
- Produzir e divulgar periodicamente informação fiável sobre o fenómeno da corrupção;
- Cooperar no plano internacional no combate à corrupção.

Da Estratégia Nacional Anticorrupção, decorre a publicação do Decreto-Lei n.º 109-E/2021, de 9 de dezembro, em vigor a partir de 7 de junho de 2022, que cria o Mecanismo Nacional Anticorrupção (MENAC) e que estabelece o Regime Geral de Prevenção da Corrupção (RGPC).

Ambos os instrumentos legais, permitem retirar do domínio da *soft law* a implementação de instrumentos como os programas de cumprimento normativo, os quais deverão incluir os planos de prevenção ou gestão de riscos, os códigos de ética e de conduta, programas de formação, os canais de denúncia e a designação de um/a responsável pelo cumprimento normativo

No âmbito da temática da anticorrupção, o Instituto de Informática, I.P., em cumprimento do Decreto-Lei n.º 109-E/2021, de 9 de dezembro, que aprova o RGPC, adotou um conjunto de medidas que incluem o Código de Ética e Conduta do Instituto, o Regulamento de Utilização da Informação, o Regulamento de Utilização de Tecnologias de Informação e Comunicação e o Código de Conduta de Fornecedores, agregados no PIT – Plano de Integridade e Transparência, nesse sentido estruturando as suas medidas num ciclo de melhoria contínua.

De realçar o artigo 5.º do RGPC, que preconiza:

- *As entidades abrangidas adotam e implementam um programa de cumprimento normativo que inclua, pelo menos, um plano de prevenção de riscos de corrupção e infrações conexas, um código de conduta, um programa de formação e um canal de denúncias, a fim de prevenirem, detetarem e sancionarem atos de corrupção e infrações conexas, levadas a cabo ou contra a entidade.*
- *As entidades designam, como elemento da direção superior ou equiparado, um responsável pelo cumprimento normativo, que garante e controla a aplicação do programa normativo.*
- *O responsável pelo cumprimento normativo exerce as suas funções de modo independente, permanente e com autonomia decisória, devendo ser assegurado, pela respetiva entidade, que dispõe da informação interna e dos meios humanos e técnicos necessários ao bom desempenho da sua função.*

2.3. Funções e Responsabilidades

A gestão do risco cabe a todos os trabalhadores, independentemente da posição que ocupem na estrutura hierárquica. No fundo, o presente plano aplica-se a todos os trabalhadores internos ou externos que integram o Instituto de Informática, I.P..

A implementação, execução e avaliação do PIT - Plano de Integridade e Transparência, será uma preocupação permanente de toda a organização, em particular dos seus dirigentes, mas será em primeira linha do Responsável de Conformidade Anticorrupção.

O Conselho Diretivo, nos termos do n.º 2 e 3 do artigo 5.º do RGPC, designou como Responsável pela Conformidade Anticorrupção, o dirigente superior Carlos Pinto, Deliberação n.º 12/CD/2022, de 28/07/2022, atribuindo-lhe a responsabilidade e delegando-lhe a autoridade necessária para assegurar o eficaz funcionamento do PIT.

INTERVENIENTES	FUNÇÕES E RESPONSABILIDADES
Responsável pela Conformidade Anticorrupção	• Responsável pelo Cumprimento normativo; • Garante e controla a aplicação do programa de cumprimento normativo.
Gestor do PIT	• Estabelece a arquitetura e os critérios da gestão de risco, promovendo a sua revisão e consolidação quando necessário. • Acompanha a execução das medidas previstas no Plano; • Contribui para a melhoria contínua do Sistema de Gestão do Risco; • Elabora os respetivos relatórios. • Revê e atualiza o Plano, sempre que necessário
Diretores de Departamento e Coordenadores de Área	• São os responsáveis pela organização, aplicação e acompanhamento do Plano na parte respetiva; • Identificar, recolher e comunicar ao Responsável pela Conformidade Anticorrupção, qualquer ocorrência de risco com provável gravidade maior; • Responsabilizam-se pela eficácia das medidas de controlo de risco na sua esfera de atuação.

2.4. Identificação dos riscos de corrupção e infrações conexas

CONCEITO DE RISCO

"*Evitar o risco é eliminar a sua causa. Preveni-lo é procurar minimizar a probabilidade da sua ocorrência ou do seu impacto negativo",* Direção-Geral do Tribunal de Contas.

Por "*risco*" ter-se-á o acontecimento, situação ou circunstância suscetível de gerar corrupção ou uma infração conexa, como consagrado na Deliberação do CPC, de 4 de março de 2009.

"*Gerir*" um risco visa o objetivo de defender e proteger cada interveniente num procedimento, e, desse modo, a salvaguarda do interesse coletivo.

Segundo a FERMA (*Federation of European Risk Management Associations*) - Norma de Gestão de Riscos (ISO 31000:2018), o termo risco designa o resultado da combinação entre a probabilidade de ocorrência de um determinado evento e o impacto resultante da sua ocorrência, positivo ou negativo, na consecução dos objetivos de uma unidade organizacional.

METODOLOGIA ADOTADA

A metodologia adotada para a identificação, avaliação e tratamento dos riscos foi definida com base na NP ISO 31000:2018, a qual contribui, entre outras coisas, para:

- Definir e alocar as principais responsabilidades assumidas na gestão do risco pelo Instituto de Informática;
- Identificar e descrever os riscos;
- Analisar os riscos identificados através da análise da probabilidade e do impacto de ocorrência do risco;
- Tratar os riscos através da definição de planos de ação;
- Registar e reportar as ações implementadas, através da análise dos resultados e da publicação e divulgação dos mesmos.

MATRIZ DE RISCO

A matriz de risco permite aferir o grau dos riscos, tendo em conta a relação estabelecida entre probabilidade e impacto do risco:

			PROBABILIDADE			
			Remoto	Possível	Alta probabilidade	Esperado
			1	2	3	4
IMPACTO	Muito alto	4	4 - Médio	8 - Alto	12 - Muito alto	16 - Muito alto
	Alto	3	3 - Médio	6 - Alto	9 - Alto	12 - Muito alto
	Médio	2	2 - Baixo	4 - Médio	6 - Alto	8 - Alto
	Baixo	1	1 - Baixo	2 - Baixo	3 - Médio	4 - Médio

Após a avaliação dos riscos, e consoante a classificação atribuída, pode ser adotada uma das seguintes estratégias, de acordo com a tabela seguinte:

Risco				
Quantitativo	Qualitativo	Classificação	Ação	Estratégia
[1 - 3[Baixo	Baixo	Sem Relevância	Sem ação	Aceitar
[3 - 6[Médio	Médio	Aceitável	Monitorar	
[6 - 12[Alto	Alto	Indesejado	Ação	Mitigar, Evitar ou Transferir/ Partilhar
[12 - 16] Muito alto	Muito Alto	Inaceitável	Ação urgente	

Por regra, os níveis de risco aceites pelo Instituto de Informática são Baixo ou Médio, com valores inferiores a 6.

MEDIDAS PREVENTIVAS DO RISCO

As medidas de prevenção a adotar que estão detalhadamente elencadas nos quadros, foram estabelecidas em função do grau de risco de corrupção e infrações conexas, com o objetivo de prevenilo ou mesmo eliminá-lo, promovendo a existência de relações mais transparentes.

ASSIM E NA PROSSECUÇÃO DESSE OBJETIVO, O INSTITUTO DE INFORMÁTICA, I.P. DEVE:
Melhorar o sistema de controlo interno, nomeadamente promovendo a elaboração de manuais de procedimentos internos pelos serviços e, concomitantemente, a sua verificação e atualização regular;
Promover, entre os seus trabalhadores, uma cultura de responsabilidade e de observação estrita de regras éticas e deontológicas e de atuação por forma a reforçar a confiança dos cidadãos na integridade, imparcialidade e eficácia dos poderes públicos;
Promover a vinculação de práticas procedimentais conformes com a lei;
Assegurar que os trabalhadores sejam conhecedores das suas obrigações, designadamente no que se refere à obrigatoriedade de denúncia de práticas suscetíveis de enquadrar ilícitos conectados com a corrupção ou a elas conducentes.

O Instituto de Informática, I.P. reavalia os riscos de corrupção e infrações conexas, por forma a considerar riscos específicos no âmbito dos seguintes processos-chave:

- Seleção de candidatos;
- Execução e verificação de operações;
- Verificação dos pagamentos;
- Adjudicação por Ajuste Direto.

A CORRUPÇÃO E AS INFRAÇÕES CONEXAS

O artigo 266.º da Constituição da República Portuguesa determina que a *Administração Publica visa a prossecução do interesse público (n.º 1) e que os Órgãos e Agentes Administrativos estão subordinados à Constituição e à Lei e devem atuar, no exercício das suas funções, com respeito pelos princípios da igualdade, da proporcionalidade, da justiça, da imparcialidade e da boa-fé* (n.º 2).

Por outro lado, o artigo 269.º também da Lei Fundamental assinala que *no exercício das suas funções, os trabalhadores da Administração Pública e demais agentes do Estado e outras entidades públicas estão exclusivamente ao serviço do interesse público* (n.º 1).

Constitui, assim, a realização do interesse público, o fim único e possível da atividade administrativa.

Subordinada à Constituição e à Lei, toda a atuação administrativa tem que obedecer aos referidos princípios da igualdade, da proporcionalidade, da justiça e da imparcialidade.

A realização de outros interesses, pessoais ou de terceiros, o tratamento preferencial ou o uso de critérios diversos na apreciação de situações idênticas, consubstanciam atos ilícitos, alguns dos quais se encontram tipificados como crimes.

São crimes cometidos no exercício de funções públicas: a *corrupção* (artigo 372.º a 374.º Código Penal (CP)), o *peculato* (artigo 375.º CP), o *peculato de uso* (artigo 376.º CP), a *participação económica em negócio* (artigo 377.º CP), a *concussão* (artigo 379.º CP), o *abuso de poder* (artigo 382.º CP) e a *violação de segredo por funcionário* (artigo 383.º CP).

Corrupção – Prática de um qualquer ato ou a sua omissão, seja lícito ou ilícito, contra o recebimento ou a promessa de uma qualquer compensação que não seja devida, para o próprio ou para terceiro.

O crime de corrupção implica a conjugação dos seguintes elementos:

- Uma ação ou omissão;
- A prática de um ato lícito ou ilícito;
- A contrapartida de uma vantagem indevida;
- Para o próprio ou para terceiro.

Pode definir-se como o desvio de um poder para fins diferentes daqueles para que foi concedido. Ou, (abuso) para fins particulares de um poder recebido por delegação.

A corrupção normalmente envolve duas ou mais pessoas que entram numa espécie de acordo secreto.

A corrupção, que etimologicamente significa apodrecimento, traduz-se num fenómeno que assume um carácter transnacional. É transversal ao sector público e privado, põe em causa os princípios fundamentais do Estado de Direito Democrático, inquina as regras da economia e compromete o normal funcionamento dos mercados, prejudicando gravemente a fluidez das relações entre os cidadãos e a Administração Pública e ocasiona o descrédito das instituições públicas.

TIPOS DE CORRUPÇÃO

A corrupção pode ser ativa ou passiva dependendo se a ação ou omissão for praticada pela pessoa que corrompe ou pela pessoa que se deixa corromper.

Por exemplo, quando alguém entrega dinheiro em troca de um favor, pratica um crime de corrupção ativa. Quando alguém recebe dinheiro para cumprir ou omitir certos atos, pratica o crime de corrupção passiva.

Corrupção ativa – Quem por si ou por interposta pessoa com o seu consentimento ou ratificação, der ou prometer a funcionário ou a terceiro com conhecimento daquele, vantagem patrimonial ou não patrimonial que ao funcionário não seja devida. (artigo 374º CP).

Exemplo: O condutor de viatura afeta ao Instituto de Informática, I.P. que intercetado por um agente da Brigada de Trânsito, em excesso de velocidade, promete àquele uma quantia monetária para não ser sancionado.

Corrupção passiva para ato ilícito - O funcionário que por si, ou por interposta pessoa com o seu consentimento ou ratificação, solicitar ou aceitar, para si ou para terceiro, sem que lhe seja devida, vantagem patrimonial ou não patrimonial, ou a sua promessa, para um qualquer ato ou omissão contrários aos deveres do cargo, ainda que anteriores àquela solicitação ou aceitação (artigo 372º do CP).

Exemplo: O trabalhador em funções públicas aceita uma vantagem económica para eliminar informaticamente o processo executivo, por dívidas à Segurança Social.

Corrupção passiva para ato lícito - O funcionário que por si, ou por interposta pessoa com o seu consentimento ou ratificação, solicitar ou aceitar, para si ou para terceiro, sem que lhe seja devida, vantagem patrimonial ou não patrimonial, ou a sua promessa, para um qualquer ato ou omissão não contrários aos deveres do cargo.

Exemplo: O trabalhador em funções públicas aceita uma vantagem económica para acelerar o pagamento de uma despesa, não respeitando as devidas prioridades.

Corrupção com prejuízo para o Comércio Internacional – Quem por si ou, mediante o seu consentimento ou ratificação, por interposta pessoa der ou prometer a funcionário, nacional, estrangeiro ou de organização internacional, ou a titular de cargo político, nacional ou estrangeiro, a terceiro com conhecimento daqueles, vantagem patrimonial ou não patrimonial, que lhe não seja devida, para obter ou conservar um negócio, um contrato ou outra vantagem indevida no comércio internacional (Artigo 7º da Lei n.º 20/2008 de 21 de abril, com a última alteração dada pela Lei n.º 30/2015, de 22 de abril)

Exemplo: O empresário que promete compensação financeira a um titular de um cargo político para que este o indique como fornecedor preferencial de um determinado produto a exportar para outro país, violando as regras da concorrência e do mercado livre.

INFRAÇÕES CONEXAS – Outros crimes prejudiciais ao bom funcionamento das instituições e dos mercados. Comum a estes crimes é a obtenção de uma vantagem ou compensação não devida.

O abuso de confiança (artigo 205.º CP), o suborno (artigo 363.º CP), o tráfico de influência (artigo 335.º CP), o peculato (artigo 375.º CP), a concussão (artigo 379.º CP), a participação económica em negócio (artigo 377.º CP) e o abuso de poder (artigo 382.º CP) são crimes próximos da corrupção e igualmente prejudiciais à ação das instituições e do mercado.

Abuso de poder – Comportamento do trabalhador que abusa de poderes ou viola deveres inerentes às suas funções, com intenção de obter, para si ou para terceiro, benefício ilegítimo ou causar prejuízo a outra pessoa.

Exemplo: O autarca que urbaniza terrenos de um familiar seu, a fim de os valorizar.

Peculato – Conduta do funcionário que ilegitimamente se apropriar, em proveito próprio ou de outra pessoa, de dinheiro ou qualquer coisa móvel, pública ou particular que lhe tenha sido entregue, esteja na sua posse ou lhe seja acessível em razão das suas funções.

Exemplo: Um trabalhador que utiliza um veículo afeto ao Instituto de Informática, I.P. para passar férias.

Participação Económica em Negócio – Comportamento do funcionário que com intenção de obter, para si ou para terceiro, participação económica ilícita, lesar em negócio jurídico os interesses patrimoniais que, no todo ou em parte, lhe cumpre, em razão da sua função, administrar, fiscalizar, defender ou realizar.

Exemplo: Funcionário responsável pelo aprovisionamento que adjudique, por preço manifestamente excessivo, serviços a uma empresa de um familiar com prejuízo para o interesse público.

Concussão – Conduta do funcionário que, no exercício das suas funções ou de poderes de facto delas decorrentes, por si ou por interposta pessoa com o seu consentimento ou ratificação, receber, para si, para o Estado ou para terceiro, mediante indução em erro ou aproveitamento de erro da vítima, vantagem patrimonial que lhe seja devida ou seja superior à devida, nomeadamente contribuição, taxa, emolumento, multa ou coima.

Exemplo: O trabalhador que ao receber documentação para instruir um processo de aquisição, cobra uma taxa não prevista na lei.

Tráfico de influência – Comportamento de quem, por si ou por interposta pessoa, com o seu consentimento ou ratificação solicitar ou aceitar, para si ou para terceiro, vantagem patrimonial ou não patrimonial, ou a sua promessa, para abusar da sua influência, real ou suposta, junto de qualquer entidade pública.

Exemplo: Funcionário que, para garantir o fornecimento de bens a uma empresa de um familiar, influencia um funcionário do Instituto de Informática, I.P. a propor a adjudicação a essa empresa.

Suborno – Pratica um ato de suborno quem convencer ou tentar convencer outra pessoa, através de dádiva ou promessa de vantagem patrimonial ou não patrimonial, a prestar falso depoimento ou declaração em processo judicial, ou a prestar falso testemunho, perícia, interpretação ou tradução, sem que estes venham a ser cometidos.

Exemplo: Um arguido tenta convencer o intérprete encarregado de traduzir para português o depoimento de uma testemunha estrangeira, a não o fazer integralmente, mediante promessa de compensação financeira.

Subjacente a todas as previsões legais está o princípio segundo o qual não deve existir qualquer compensação ou vantagem não devida ou mesmo mera promessa desta, em benefício do próprio ou de terceiro, para o assumir de um determinado comportamento, seja lícito ou ilícito, através de uma ação ou uma omissão.

Deve ter-se em atenção que as infrações penais em destaque podem traduzir-se em infrações disciplinares.

A Lei Geral do Trabalho em Funções Públicas (LTFP), aprovada pela Lei n.º 35/2014, de 20 de junho, com entrada em vigor em 1 de agosto de 2014, e que veio revogar entre outros, o anterior Estatuto Disciplinar dos Trabalhadores que exercem Funções Públicas (ED), aprovado pela Lei n.º 58/2008, de 9 de setembro, contém, de resto, várias disposições legais relacionadas especificamente com a corrupção e respetivas sanções.

A pena disciplinar de suspensão é suscetível de ser aplicada a trabalhador que dispense tratamento de favor a determinada entidade, singular ou coletiva (al. e) do artigo 186.º da LTFP) e bem assim que viole, com culpa grave ou dolo, o dever de imparcialidade no exercício das funções (al. l) do artigo 186.º da LTFP).

As penas de demissão e de despedimento são aplicáveis em caso de trabalhador que, em resultado da função que exerce, solicite ou aceite, direta ou indiretamente, dádivas, gratificações, participações em lucros ou outras vantagens patrimoniais, ainda que sem o fim de acelerar ou retardar qualquer serviço ou procedimento (art.º 187º e alínea j) do n.º 3 do art.º 297.º, ambos da LTFP).

O procedimento disciplinar é independente do procedimento criminal, tanto que a condenação em processo penal não prejudica o exercício da ação disciplinar quando a infração penal constitua também infração disciplinar e quando o facto apreciado em procedimento disciplinar seja passível de ser considerado infração penal, dá-se obrigatoriamente notícia dele ao Ministério Público para promover o procedimento criminal, nos termos do artigo 242.º do Código de Processo Penal. (n.º 4 do art.º 179º da LTFP).

2.5. Conflito de Interesses

De acordo com a **Recomendação do CPC de 7 de novembro de 2012**, a questão de conflitos de interesses no setor público tem vindo a assumir um lugar de destaque em Portugal e na Comunidade Internacional, a par da problemática da Corrupção.

O "*conflito de interesses*" tem sido definido como qualquer situação em que o agente público, por força do exercício das suas funções, ou por causa delas, tenha de tomar decisões ou tenha contacto com procedimentos administrativos de qualquer natureza que possam afetar ou em que possam estar em causa, interesses particulares, seus ou de terceiros e que por essa via prejudiquem ou possam prejudicar a isenção e o rigor das decisões administrativas que tenham de ser tomadas, ou que possam suscitar a mera dúvida sobre a isenção e rigor que são devidos ao exercício de funções públicas.

MEDIDAS ESPECÍFICAS DE PREVENÇÃO DE CONFLITO DE INTERESSES
Manuais de boas práticas e códigos de conduta.
Identificação de potenciais situações de conflitos de interesses.
Identificação de situações que possam dar origem a um conflito real, aparente ou potencial de interesses que envolvam trabalhadores que deixaram o cargo público para exercerem funções privadas.
Identificação e caracterização de áreas de risco nomeadamente as que resultem das situações de acumulação de funções.
Promoção de comportamentos ativos de recusa de contacto e processamento relativo a procedimentos administrativos em que, sob qualquer forma, tenham um interesse.
Subscrição por todos os trabalhadores de declarações de conflitos de interesse relativamente a cada procedimento que lhe seja confiado no âmbito das suas funções e no qual, de algum modo tenha influência.
Subscrição por todos os funcionários que se encontrem em regime de acumulação de funções, de uma declaração atualizada em que assumam de forma inequívoca que as funções acumuladas não colidem sob forma alguma com as funções públicas que exercem, nem colocam em causa a isenção e o rigor que deve pautar a sua ação.
Declarações relativas a ofertas no exercício das funções.

2.6. Denúncia de Situações de Corrupção

A corrupção, enquanto crime público que é, impõe às autoridades competentes a obrigação de investigar logo que tenham notícia do crime, quer através de denúncia quer de outra forma.

E por sua vez todo e qualquer trabalhador da Administração Pública tem o dever legal de denúncia do cometimento de infrações de que tenha conhecimento no exercício dessas funções ou por causa delas, beneficiando das garantias *dos denunciantes,* previstas no artigo 4.º da Lei n.º 19/2008, de 21 de abril, com a última alteração dada pela Lei n.º 30/2015, de 22 de abril.

A denúncia pode ser feita: à Polícia Judiciária, ao Ministério Público ou a qualquer outra autoridade judiciária ou policial, verbalmente ou por escrito e não está sujeita a qualquer formalidade especial.

Poderá ainda, num futuro próximo, ser feita através do Canal de Denúncia do Instituto de Informática, I.P., disponível na intranet e na página oficial da internet.

No caso de denúncia de um crime de corrupção, esta pode ainda ser efetuada eletronicamente, através da página *online* da Procuradoria-Geral da República (https://simp.pgr.pt/dciap/denuncias/). A eventual omissão do dever de denúncia ou participação gera responsabilidade disciplinar e/ou penal consoante a gravidade da situação omitida.

2.7. Quadros Identificação, Análise e Avaliação dos Riscos

IDENTIFICAÇÃO DO RISCO									ANALISE E AVALIAÇÃO DO RISCO						
ID RISCO	DATA DO REGISTO	RESPONSÁVEL DO RISCO	DEPARTAMENTO	DESCRIÇÃO DO RISCO	CONTROLOS IMPLEMENTADOS	CATEGORIA DO RISCO	EVIDÊNCIAS DA IMPLEMENTAÇÃO	É EFICAZ?	GRAVIDADE	IMPACTO	PROBABILIDADE	VALOR DA PROBABILIDADE	NÍVEL DE RISCO	CLASSIFICAÇÃO	AÇÃO
PIT_01	02.02.2024	Helga Beirão	DOGP	Existência de conflitos de interesses que ponham em causa a transparência dos procedimentos (Júri e Gestão de contratos) - Nas Atividades do Processo G. Aquisições - Análise do Processo de Aquisição [Intervenientes - Todos os Departamentos]	- DICI	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_02	02.02.2024	Helga Beirão	DOGP	Falsas declarações prestadas pelos fornecedores (Ex: declaração de não divida; certificações) - Nas Atividades do Processo G. Aquisições - Análise do Processo de Aquisição [Intervenientes - ACP]	- Anexo I do CCP	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_03	02.02.2024	Helga Beirão	DOGP	Duplo Financiamento dos projetos - Nas Atividades do Processo G. Financeira e Orçamental - Operações Cofinanciadas [Intervenientes - CD/AFA]	- Diferenciação de fundos orçamentais com controlo e execução autonomos. - Contas bancárias independentes para gestão das operações cofinanciadas	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_04	02.02.2024	Helga Beirão	DOGP	Utilização indevida de financiamento (para um fim diferente do objeto da candidatura/contrato) - Nas Atividades do Processo G. Aquisições - Análise do Processo de Aquisição [Intervenientes - CD/AFA]	- Afetação ao fundo orçamental respetivo desde o início - Funcionamento do sistema financeiro (não permite pagamentos para outros fins)	Risco Reputacional	Sim	Sim	Alto	Alto	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Médio	Aceitável	Monitorar
PIT_05	02.02.2024	Helga Beirão	DOGP	Insuficiente justificação para adoção de procedimentos por ajuste direto, consulta prévia e critérios materiais - Nas Atividades do Processo G. Aquisições - Análise do Processo de Aquisição [Intervenientes - Todos os Departamentos]	Preenchimento adequado da Informação de Necessidade de Aquisição (MOD223)	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_06	02.02.2024	Helga Beirão	DOGP	Incumprimento do Artº 113 do CCP no âmbito de Procedimentos por Ajuste Direto e Consulta Prévia - Nas Atividades do Processo G. Aquisições - Análise do Processo de Aquisição [Intervenientes - ACP]	- Plataforma Acingov	Risco de Conformidade	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_07	02.02.2024	Helga Beirão	DOGP	Admissão de propostas extemporâneas ou de entidades com impedimentos legais - Nas Atividades do Processo G. Aquisições - Análise do Processo de Aquisição [Intervenientes - Juris dos procedimentos]	- Plataforma Acingov - Análise dos documentos de habilitação	Risco Operacional	Sim	Sim	Médio	Médio	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_08	02.02.2024	Helga Beirão	DOGP	Favorecimento de fornecedores - Nas Atividades do Processo G. Aquisições [Intervenientes - Juris dos procedimentos]	- Cumprimento do CCP - PIT	Risco Reputacional	Sim	Sim	Médio	Médio	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_09	02.02.2024	Helga Beirão	DOGP	Tráfico de influências - Nas Atividades do Processo G. Aquisições [Intervenientes - Todos os Departamentos, Assessoria Jurídica e CD]	- Adoção preferencial de procedimento concorrenciais (com juris de procedimento) - DICI - PIT	Risco Reputacional	Sim	Sim	Médio	Médio	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_10	02.02.2024	Helga Beirão	DOGP	Assunção de despesas sem cabimento prévio - Nas Atividades do Processo G. Financeira e Orçamental [Intervenientes - CD/AFA]	- Processo de aprovação de despesa (condiciona a aprovação à existência de cabimento obrigatório)	Risco Operacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação

IDENTIFICAÇÃO DO RISCO									ANALISE E AVALIAÇÃO DO RISCO						
ID RISCO	DATA DO REGISTO	RESPONSÁVEL DO RISCO	DEPARTAMENTO	DESCRIÇÃO DO RISCO	CONTROLOS IMPLEMENTADOS	CATEGORIA DO RISCO	EVIDÊNCIAS DA IMPLEMENTAÇÃO	É EFICAZ?	GRAVIDADE	IMPACTO	PROBABILIDADE	VALOR DA PROBABILIDADE	NÍVEL DE RISCO	CLASSIFICAÇÃO	AÇÃO
PIT_11	02.02.2024	Helga Beirão	DOGP	Incumprimento do direito de audiência prévia - Nas Atividades do Processo G. Aquisições - Análise do Processo de Aquisição [Intervenientes - Juris dos procedimentos]	- Cumprimento do CCP - Acingov	Risco de Conformidade	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_12	02.02.2024	Helga Beirão	DOGP	Inexistência de segregação de funções (nas diferentes fases do ciclo de despesa, na tramitação do processo aquisitivo e na execução do contrato) - Nas Atividades do Procedimento de Autorização de Exceção de Segregação de Funções [Intervenientes - Todos]	- Segregação de funções	Risco Operacional	Sim	Sim	Médio	Médio	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_13	02.02.2024	Helga Beirão	DOGP	Incumprimento do princípio da concorrência - Nas Atividades do Processo G. Aquisições - Gestão de Aquisições em Regime Simplificado/Não Simplificado [Intervenientes - ACP]	- Cumprimento do CCP	Risco de Conformidade	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_14	02.02.2024	Helga Beirão	DOGP	Descricionariedade na avaliação das propostas/candidaturas - Nas Atividades do Processo G. Aquisições [Intervenientes - Juris dos procedimentos]	- Critérios de adjudicação definidos nas Peças dos Procedimentos	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_15	02.02.2024	Helga Beirão	DOGP	Elaboração de peças procedimentais com requisitos passíveis de privilegiar ou excluir determinadas entidades - Nas Atividades do Processo G. Aquisições - Gestão de Aquisições em Regime Simplificado/Não Simplificado [Intervenientes - Todos os Departamentos e Assessoria Jurídica]	- Critérios de adjudicação definidos nas Peças dos Procedimentos - Multidisciplinaridade na elaboração das peças - Definição dos atributos da proposta	Risco Operacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_16	02.02.2024	Helga Beirão	DOGP	Manipulação de procedimentos concursais - Nas Atividades do Processo G. Aquisições - Gestão de Aquisições em Regime Simplificado/Não Simplificado [Intervenientes - ACP e Serviços Requisitantes]	- Critérios de adjudicação definidos nas Peças dos Procedimentos - Multidisciplinaridade na elaboração das peças - Definição dos atributos da proposta	Risco de Conformidade	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_17	02.02.2024	Helga Beirão	DOGP	Deficiente ou insuficiente definição dos critérios de adjudicação ou qualificação - Nas Atividades do Processo G. Aquisições - Gestão de Aquisições em Regime Simplificado/Não Simplificado [Intervenientes - Todos os Departamentos e Assessoria Jurídica]	- Critérios de adjudicação definidos nas Peças dos Procedimentos - Multidisciplinaridade na elaboração das peças - Definição dos atributos da proposta	Risco Operacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_18	02.02.2024	Helga Beirão	DOGP	Deficiente ou insuficiente definição das cláusulas de penalização contratuais em caso de não cumprimento das obrigações por ambas as partes - Nas Atividades do Processo G. Aquisições - Gestão de Aquisições em Regime Simplificado/Não Simplificado [Intervenientes - ACP e Assessoria Jurídica]	- Multidisciplinaridade na elaboração das peças - Definição dos atributos da proposta	Risco Operacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_19	02.02.2024	Helga Beirão	DOGP	Falta de correspondência entre as cláusulas contratuais e as definidas nas peças do respetivo concurso - Nas Atividades do Processo G. Aquisições - Aceitação do Contrato [Intervenientes - ACP e Assessoria Jurídica]	- Minuta contratual remete para as cláusulas do Caderno de Encargos	Risco Operacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_20	02.02.2024	Helga Beirão	DOGP	Deficiente controlo e validação da execução do contrato - Nas Atividades do Processo G. Aquisições - Gestão de Fornecedores e Contratos [Intervenientes - Gestor do Contrato]	- Nomeação de Gestores de Contrato	Risco Operacional	Sim	Sim	Médio	Médio	Possível - Possível de ocorrer (10% - 50%)	Médio	Médio	Aceitável	Monitorar

IDENTIFICAÇÃO DO RISCO									ANALISE E AVALIAÇÃO DO RISCO						
ID RISCO	DATA DO REGISTO	RESPONSÁVEL DO RISCO	DEPARTAMENTO	DESCRIÇÃO DO RISCO	CONTROLOS IMPLEMENTADOS	CATEGORIA DO RISCO	EVIDÊNCIAS DA IMPLEMENTAÇÃO	É EFICAZ?	GRAVIDADE	IMPACTO	PROBABILIDADE	VALOR DA PROBABILIDADE	NÍVEL DE RISCO	CLASSIFICAÇÃO	AÇÃO
PIT_21	02.02.2024	Helga Beirão	DOGP	Avaliação de fornecedores deficiente ou inexistente - Nas Atividades do Processo G. Aquisições - Gestão de Fornecedores e Contratos [Intervenientes - Gestor do Contrato]	- Manual de Avaliação de Fornecedores	Risco Operacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_22	02.02.2024	Helga Beirão	DOGP	Inadequada definição do preço base (sem considerar critérios objetivos) - Nas Atividades do Processo G. Aquisições - Análise do Processo de Aquisição [Intervenientes - ACP e Serviços Requisitantes]	- Fundamentação obrigatória à luz do CCP	Risco de Conformidade	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_23	02.02.2024	Helga Beirão	DOGP	Manipulação da faturação - Nas Atividades do Processo G. Aquisições [Intervenientes - AFA]	- Segregação de funções - RPA implementado para tratamento das faturas recebidas no II - Circuito de validação de faturas	Risco de Conformidade	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_24	02.02.2024	Helga Beirão	DOGP	Fracionamento de despesa - Nas Atividades do Processo G. Aquisições [Intervenientes - Todos os Departamentos e CD]	- Definição clara do objeto dos contratos - Plano anual de compras	Risco Reputacional	Sim	Sim	Médio	Médio	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_25	02.02.2024	Helga Beirão	DOGP	Desvio ou não fiscalização da quantidade e qualidade dos bens e serviços (Trabalhos, bens /serviços não fornecidos ou substituidos) - Nas Atividades do Processo G. Aquisições - Gestão de Fornecedores e Contratos [Intervenientes - Gestor do Contrato e Departamentos com responsabilidade na gestão do inventário]	- Nomeação de Gestores de Contrato - Manual de avaliação de fornecedores	Risco Operacional	Sim	Sim	Médio	Médio	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_26	02.02.2024	Helga Beirão	DOGP	Realização de alterações contratuais, sem dar cumprimento ao definido nas regras da contratação pública - Nas Atividades do Processo G. Aquisições - Gestão de Disputas Contratuais [Intervenientes - ACP, Assessoria Jurídica e Gestor do Contrato]	- Cumprimento do CCP	Risco de Conformidade	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_27	02.02.2024	Helga Beirão	DOGP	Práticas de dumping - Nas Atividades do Processo G. Aquisições [Intervenientes - ACP]	- Cumprimento do CCP	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_28	02.02.2024	Helga Beirão	DOGP	Insuficiências ao nível da inventariação e avaliação contabilística dos bens - Nas Atividades do Processo G. Financeira e Orçamental - Gestão de Património [Intervenientes - AFA]	- Cumprimento do SNCAP - SIF	Risco Operacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_29	02.02.2024	Helga Beirão	DOGP	Desadequada gestão de inventário de equipamentos informáticos - Nas Atividades do Processo G. Financeira e Orçamental - Gestão de Património [Intervenientes - AFA]	- SIF - Ferramenta de ITSM (DAU/DAS)	Risco Operacional	Sim	Sim	Alto	Alto	Possível - Possível de ocorrer (10% - 50%)	Médio	Alto	Indesejado	Ação
PIT_30	02.02.2024	Helga Beirão	DOGP	Retenção de material para uso próprio do trabalhador - Nas Atividades do Procedimento de Entrada e Saída de Colaboradores [Intervenientes - Todos]	- Procedimento de Entrada e Saída de Colaboradores - Reporte trimestral de indicadores do procedimento	Risco Operacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação

IDENTIFICAÇÃO DO RISCO									ANALISE E AVALIAÇÃO DO RISCO						
ID RISCO	DATA DO REGISTO	RESPONSÁVEL DO RISCO	DEPARTAMENTO	DESCRIÇÃO DO RISCO	CONTROLOS IMPLEMENTADOS	CATEGORIA DO RISCO	EVIDÊNCIAS DA IMPLEMENTAÇÃO	É EFICAZ?	GRAVIDADE	IMPACTO	PROBABILIDADE	VALOR DA PROBABILIDADE	NÍVEL DE RISCO	CLASSIFICAÇÃO	AÇÃO
PIT_31	02.02.2024	Helga Beirão	DOGP	Processo de validação de despesa incompleto ou desadequado - Nas Atividades do Processo G. Financeira e Orçamental [Intervenientes - AFA]	- Processo de G. Financeira e Orçamental	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_32	02.02.2024	Helga Beirão	DOGP	Incumprimento, por dolo ou negligência, das obrigações fiscais - Nas Atividades do Processo G. Financeira e Orçamental [Intervenientes - AFA]	- Procedimentos internos instituidos (fecho de mês)	Risco de Conformidade	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_33	02.02.2024	Helga Beirão	DOGP	Favorecimento no âmbito de processos de recrutamento de recursos humanos. - Nas Atividades do Processo G. Pessoas Recrutamento e seleção [Intervenientes - AGP e CD]	- Juris de procedimento - Vários intervenientes no procedimento de contratação	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_34	02.02.2024	Helga Beirão	DOGP	Recurso a trabalho suplementar, contratações a termo ou a prestações de serviços, como forma de suprir necessidades permanentes dos serviços. - Nas Atividades do Processo G. Pessoas - Gestão Administrativa de Pessoal [Intervenientes - AGP e CD]	- Plano Anual de Recrutamento - Regulamento carreiras CIT (formas de contratação mais ágeis e mais competitivas com o mercado)	Risco Reputacional	Sim	Sim	Médio	Médio	Possível - Possível de ocorrer (10% - 50%)	Médio	Médio	Aceitável	Monitorar
PIT_35	02.02.2024	Helga Beirão	DOGP	Acumulação ilegítima de funções - Nas Atividades do Processo G. Pessoas - Gestão Administrativa de Pessoal [Intervenientes - Todos]	- Verificação semestral do cumprimento de acumulação de funções - Reporte anual ao Tribunal de Contas	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_36	02.02.2024	Helga Beirão	DOGP	Irregularidades/falhas no processamento de vencimentos e abonos dos trabalhadores. - Nas Atividades do Processo G. Pessoas - Gestão Administrativa de Pessoal [Intervenientes - AGP]	- Segregação de funções	Risco de Conformidade	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_37	02.02.2024	Helga Beirão	DOGP	Ações de formação para trabalhadores em funções públicas, realizadas por entidades privadas a título gratuito para obter vantagens ilícitas. - Nas Atividades do Processo G. Pessoas - Formação e Desenvolvimento de Competências [Intervenientes - ACP e AGP]	- Código de Ética e Conduta - CPP	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_38	02.02.2024	Helga Beirão	DOGP	Recurso a formação prestada por entidades privadas não acreditadas. - Nas Atividades do Processo G. Pessoas - Formação e Desenvolvimento de Competências [Intervenientes - AGP, ACP e CD]	- Exigência de comprovativo de acreditação no processo de aquisição	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_39	02.02.2024	Helga Beirão	DOGP	Existência de conflitos de interesses que ponham em causa a transparência dos procedimentos de avaliação de desempenho. - Nas Atividades do Processo G. Pessoas - Avaliação de Desempenho [Intervenientes - Todos os Avaliadores, AGP e Comissão de Avaliação de Desempenho]	- Os trabalhadores são avaliados pelo seu dirigente, que não concorre para as mesmas quotas	Risco de Conformidade	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_40	02.02.2024	Helga Beirão	DOGP	Exercício ilegal da discricionariedade no processo de avaliação dos trabalhadores. - Nas Atividades do Processo G. Pessoas - Avaliação de Desempenho [Intervenientes - Todos os Avaliadores, AGP e Comissão de Avaliação de Desempenho]	- Várias instâncias de decisão no processo de avaliação (os trabalhadores podem reclamar, recorrer)	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação

IDENTIFICAÇÃO DO RISCO									ANALISE E AVALIAÇÃO DO RISCO						
ID RISCO	DATA DO REGISTO	RESPONSÁVEL DO RISCO	DEPARTAMENTO	DESCRIÇÃO DO RISCO	CONTROLOS IMPLEMENTADOS	CATEGORIA DO RISCO	EVIDÊNCIAS DA IMPLEMENTAÇÃO	É EFICAZ?	GRAVIDADE	IMPACTO	PROBABILIDADE	VALOR DA PROBABILIDADE	NÍVEL DE RISCO	CLASSIFICAÇÃO	AÇÃO
PIT_41	02.02.2024	Helga Beirão	DOGP	Prestação de falsas declarações (em momento de Acidentes de Trabalho "in itinarae") - Nas Atividades do Processo G. Pessoas - Segurança e Saúde no Trabalho [Intervenientes - Todos]	- Subprocesso de Acidentes de Trabalho - Preenchimento dos modelos de declaração de acidente - Entrega de documentos comprovativos (declaração médica de atesta o acidente de trabalho)	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_42	02.02.2024	Helga Beirão	DOGP	Interferência ilegal nas bases de dados pessoais dos trabalhadores em funções públicas - Nas Atividades do Processo G. Pessoas - Gestão Administrativa de Pessoal [Intervenientes - AGP]	- Gesven (controlo de rastreamento e de acesso às BDs)	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_43	23.02.2024	Nuno Miranda	DAS	Manipulação de dados/fornecimento de informação a terceiros/abuso de confiança/favorecimento próprio ou de terceiros - Nas Atividades do Segurança da Informação [Intervenientes - Todos]	Políticas de Segurança da Informação	Risco Operacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_44	23.02.2024	Célia Vasconcelos	AQA	Deficiente/inexistente acompanhamento das ações corretivas/de melhoria a implementar (decorrentes de auditorias ou avaliações). - Nas Atividades do Auditoria/Controlo interno [Intervenientes - AQA]	Dashboard/Tabela de Ações Corretivas e de Melhoria; reuniões da Comissão da Qualidade; Relatórios de monitorização das ACM	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_45	23.02.2024	Célia Vasconcelos	AQA	Ausência de independência/ neutralidade na realização de auditorias internas em função de outros interesses e/ou em conivência com os auditados. - Nas Atividades do Auditoria/Controlo interno [Intervenientes - AQA]	Procedimento de Auditorias Internas; Segregação da função de auditoria face às restantes atividades; Análise, validação e aprovação a vários níveis	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_46	23.02.2024	Nuno Miranda	DAS	Utilização de informação privilegiada para benefício próprio ou de terceiros - Nas Atividades do Segurança da Informação [Intervenientes - Todos]	Políticas de Segurança da Informação; Procedimentos de controlo e gestão de acessos; Acordos de confidencialidade; Procedimento de Monitorização de Logs	Risco Reputacional	Sim	Sim	Baixo	Baixo	Remoto – Possibilidade remota de acontecer (<10%)	Baixo	Baixo	Sem Relevância	Sem Ação
PIT_47	27.02.2024	CD	Todos	Possibilidade de acumulação de vários papéis numa mesma pessoa ao longo do ciclo do investimento - Nas atividades do Processo de G. Aquisições e do Processo de G. Financeira e Orçamental [Intervenientes - Todos]	- Segregação de funções - Matriz RACI dos Processos - Código de Ética e Conduta	Risco Reputacional	Sim	Não	Alto	Alto	Possível - Possível de ocorrer (10% - 50%)	Médio	Alto	Indesejado	Sem Ação

O detalhe pormenorizado da análise e avaliação dos riscos acima identificados, encontra-se arquivado, em formato digital, na pasta respetiva do repositório de ficheiros do responsável pela elaboração desta análise, no Instituto de Informática.

Tratamento dos Riscos (Tabela de Ações a Implementar)

Face aos riscos identificados, a estratégia definida foi a de Mitigação. Para isso, apresentam-se abaixo as ações de tratamento dos riscos identificados acima.

ID RISCO	DESCRIÇÃO DO RISCO	AÇÃO A IMPLEMENTAR	RESPONSÁVEL DA AÇÃO	PRAZO DE IMPLEMENTAÇÃO
PIT_20	Deficiente controlo e validação da execução do contrato - Nas Atividades do Processo G. Aquisições - Gestão de Fornecedores e Contratos [Intervenientes - Gestor do Contrato]	Sensibilizar os Gestores de Contrato para uma maior eficiência na gestão dos contratos	Susana Gamito	31.12.2024
PIT_28	Insuficiências ao nível da inventariação e avaliação contabilística dos bens - Nas Atividades do Processo G. Financeira e Orçamental - Gestão de Património [Intervenientes - AFA]	Reforço do controlo de gestão de ativos	Catarina F. Martins	31.12.2024
PIT_29	Desadequada gestão de inventário de equipamentos informáticos - Nas Atividades do Processo G. Financeira e Orçamental - Gestão de Património [Intervenientes - AFA]	Realizar ações de sensibilização no âmbito da responsabilização pela segurança dos ativos	Helga Beirão/ Sergio Duarte	31.12.2024
PIT_47	Possibilidade de acumulação de vários papéis numa mesma pessoa ao longo do ciclo do investimento - Nas atividades do Processo de G. Aquisições e do Processo de G. Financeira e Orçamental [Intervenientes - Todos]	Realizar periodicamente sessões de sensibilização acerca da conveniência da repartição das tarefas e responsabilidades nas diversas fases procedimentais de processos de contratação pública, desde a sua génese, com a identificação das necessidades até ao respetivo pagamento.	CD	29.12.2024

2.8. Quadro Legal

Legislação Internacional

No sentido de prevenir e combater a corrupção têm sido adotados, nos últimos anos, vários instrumentos jurídicos internacionais aos quais Portugal aderiu, nomeadamente:

- A Convenção Relativa à Luta Contra a Corrupção em que estejam implicados Funcionários das Comunidades Europeias ou dos Estados-membros da União Europeia

  Assinada em Bruxelas em 26/5/1997, aprovada pela Resolução da Assembleia da República n.º 72/2001, de 20/9, e ratificada pelo Estado Português através do Decreto do Presidente da República n.º 58/2001, de 15/11/2001 (DR, Série I-A, n.º 265, de 15/11/2001).

- A Convenção sobre a Luta Contra a Corrupção de Agentes Públicos Estrangeiros nas Transações Comerciais Internacionais

  Adotada em Paris em 17/12/1997, na Conferência Ministerial da Organização de Cooperação e de Desenvolvimento Económico (OCDE), transposta para o direito interno pela Lei n.º 13/2001, de 4/7.

- A Convenção Penal Contra a Corrupção do Conselho da Europa

  Assinada em Estrasburgo a 30/04/1999, aprovada pela Resolução da Assembleia da República n.º 68/2001, de 20/9, e ratificada pelo Estado Português através do Decreto do Presidente da República n.º 56/2001, de 26/10 (DR, Série I-A, n.º 249, de 26/10/2001).

- A Convenção das Nações Unidas Contra a Corrupção

  Adotada pela Assembleia Geral das Nações Unidas em 31/10/2003, aprovada pela Resolução da Assembleia da República n.º 47/2007, de 19/7, e ratificada pelo Estado Português através do Decreto do Presidente da República n.º 97/2007, de 21/9 (DR, II Série, n.º 183, de 21/09/2007).

Legislação Nacional

O combate ao crime de corrupção faz-se quer através da previsão e punição dos comportamentos que devem ser qualificados como corrupção (direito substantivo), quer através das regras que regulam o processo penal (direito adjetivo).

O Decreto-Lei n.º 109-E/2021, de 9 de dezembro, criou o Mecanismo Nacional Anticorrupção (MENAC) e aprovou o Regime Geral de Prevenção da Corrupção (RGPC).

O Código Penal prevê, no Título V (Dos crimes contra o Estado), não só o crime de corrupção, mas também todo um conjunto de crimes conexos igualmente prejudiciais ao bom funcionamento das instituições e dos mercados. O elemento comum a todos estes crimes é a obtenção de uma vantagem (ou compensação) não devida.

Assim, no Capítulo IV (Dos crimes cometidos no exercício de funções públicas), nos artigos 372.º a 374.º-B, são previstos e punidos os vários crimes de corrupção e crimes conexos.

Em **legislação avulsa** o combate à corrupção é feito, entre outros, nos seguintes diplomas:

- A **Lei n.º 34/87, de 16 de julho**, com a última alteração dada pela Lei n.º 30/2015, de 22 de abril, determina os crimes de responsabilidade dos titulares de cargos políticos ou de altos cargos públicos, em especial o artigo 16.º (recebimento indevido de vantagem), os artigos 17.º e 18.º (corrupção passiva e ativa), os artigos 20.º a 22.º (peculato), o artigo 23.º (participação económica em negócio) e o artigo 26.º (abuso de poderes).
- A **Lei n.º 15/2001, de 5 de junho**, que aprova o regime geral das infrações tributárias, refere a corrupção como circunstância agravante, nos crimes aduaneiros (alínea d) do artigo 97.º), nos crimes fiscais (alíneas c) e d) do artigo 104.º), e nos crimes contra a segurança social (n.º 3 do artigo 106.º).
- A **Lei n.º 50/2007, de 31 de agosto**, com a última alteração dada pela Lei n.º 30/2015, de 22 de abril, estabelece um novo regime de responsabilidade penal por comportamentos suscetíveis de afetar a verdade, a lealdade e a correção da competição e do seu resultado na atividade desportiva (revoga o Decreto-Lei n.º 390/91, de 10 de outubro, com exceção do artigo 5.º), em especial os artigos 8.º e 9.º (corrupção passiva e ativa), o artigo 10.º (tráfico de influências) e o artigo 11.º (associação criminosa).
- O **Decreto-Lei n.º 18/2008, de 29 de janeiro**, que aprova o Código dos Contratos Públicos, estabelecendo a disciplina aplicável à contratação pública, determina a impossibilidade de serem candidatos, concorrentes ou integrar qualquer agrupamento, as entidades que tenham sido condenadas por sentença transitada em julgado pelo crime de corrupção (Artigo 55.º).
- A **Lei n.º 20/2008, de 21 de abril**, com a última alteração dada pelo Decreto-Lei 214-G/2015, de 2 de outubro, cria o novo regime penal de corrupção no comércio internacional e no setor privado, dando cumprimento à Decisão Quadro n.º 2003/568/JAI, do Conselho, de 22 de julho, em especial o artigo 7.º (corrupção ativa com prejuízo do comércio internacional) e os artigos 8.º e 9.º (corrupção ativa e passiva no setor privado).

No âmbito do **direito processual penal**, além das normas gerais previstas no Código de Processo Penal sobre os meios de prova, meios de obtenção de prova e realização do inquérito, existe também legislação avulsa especificamente aplicada no combate ao crime de corrupção:

- A **Lei n.º 36/94, de 29 de setembro**, com a última alteração dada pela Lei n.º 32/2010, de 2 de setembro, definiu medidas de combate à corrupção e criminalidade económica e financeira, prevendo medidas e instrumentos suscetíveis de garantirem uma ação mais eficaz a nível da prevenção e da repressão deste tipo de criminalidade.
- A **Lei n.º 5/2002, de 11 de janeiro**, com a última alteração dada pela Lei n.º 55/2015, de 23 de junho, estabelece novas medidas de combate à criminalidade organizada e económico-financeira, em resultado da constatação da insuficiência dos mecanismos existentes de combate a este tipo de criminalidade. Introduziu mecanismos de investigação e de repressão mais eficazes estabelecendo medidas especiais em matéria de derrogação do segredo fiscal

e das entidades financeiras, de registo de voz e imagem enquanto meio de prova e de perda em favor do Estado das vantagens do crime.

- A **Lei n.º 93/99, de 14 de julho**, com a última alteração dada pela Lei n.º 42/2010, de 3 de setembro, que regula a aplicação de medidas para proteção de testemunhas em processo penal, refere o crime de corrupção e crimes conexos como uma das condições para a não revelação da identidade da testemunha (artigo 16.º).
- A **Lei n.º 101/2001, de 25 de agosto**, com a última alteração dada pela Lei n.º 61/2015, de 24 de junho, aprova o regime jurídico das ações encobertas para fins de prevenção e investigação criminal, veio dar mais possibilidades legais para a obtenção de prova, estabelecendo a admissibilidade de ações encobertas no âmbito da prevenção e repressão dos crimes de corrupção, peculato, participação económica em negócio e tráfico de influências.
- A **Lei n.º 49/2008, de 27 de agosto**, com a última alteração dada pela Lei n.º 57/2015, de 23 de junho, aprova a Lei de Organização da Investigação Criminal, refere no artigo 7.º que é da competência reservada da Polícia Judiciária, não podendo ser deferida a outros órgãos de polícia criminal, a investigação, entre outros, dos crimes tráfico de influência, corrupção, peculato e participação económica em negócio, bem como de crimes com estes conexos. Por sua vez, a Lei Orgânica da Polícia Judiciária (**Lei n.º 37/2008, de 6 de agosto**) prevê a criação da Unidade Nacional de Combate à Corrupção (UNCC) com competências em matéria de prevenção, deteção, investigação criminal e a coadjuvação das autoridades judiciárias relativamente aos crimes de corrupção, peculato, tráfico de influências e participação económica em negócio.

Em matéria específica de controlo de conflitos de interesses, o ordenamento jurídico português dispõe dos seguintes instrumentos normativos que comtemplam este assunto:

- **Constituição da República Portuguesa (CRP)** relativa à responsabilidade, aos estatutos e ao regime dos funcionários da Administração Pública.
- **Código do Procedimento Administrativo (CPA).**
- **Decreto-Lei n.º 11/2012 de 20 de janeiro** - Regime de incompatibilidades do pessoal de livre designação por titulares de cargos políticos.
- **Lei n.º 64/93 de 26 de agosto (c/alterações)** - Regime jurídico de incompatibilidades e impedimentos dos titulares de cargos políticos e altos cargos públicos.
- **Lei n.º 2/2004 de 15 de janeiro**, republicada pela Lei n.º 64/2011 de 22 de dezembro - Estatuto do pessoal dirigente dos serviços e organismos da Administração central regional e local do Estado.
- **Lei n.º 35/2014 de 20 de junho,** com a última alteração da Lei n.º 84/2015, de 7 de agosto - Lei Geral do Trabalho em Funções Públicas.

2.9. Acompanhamento e Avaliação do Plano

Execução e Controlo do Plano

Para que o Plano cumpra a sua função é necessário o seu acompanhamento de forma dinâmica e a supervisão constante das atividades desenvolvidas no Instituto de Informática, I.P..

Os dirigentes desempenham um papel fundamental na prevenção e na deteção da corrupção e infrações conexas, cabendo-lhes sobretudo supervisionar ativamente os seus trabalhadores.

A execução do plano está sujeita a controlo e verificação efetuado através da elaboração de relatórios de avaliação previstos na lei em vigor, contendo nomeadamente a quantificação do grau de implementação das medidas preventivas e/ou corretivas identificadas, bem como a previsão da sua plena implementação.

De acordo com o previsto nas alíneas *a)* e *b)* do n.º 4 do artigo 6.º do RGPC, o controlo é efetuado através do relatório intercalar e do relatório anual nos seguintes termos:

- Elaboração, no mês de outubro, de relatório de avaliação intercalar nas situações identificadas de risco alto ou muito alto.
- Elaboração, no mês de abril do ano seguinte a que respeita a execução, de relatório de avaliação anual, contendo nomeadamente a quantificação do grau de implementação das medidas preventivas e corretivas identificadas, bem como a previsão da sua implementação.

Para efeitos do exercício de controlo e verificação, o Gestor do PIT apresenta ao Responsável pela Conformidade Anticorrupção o relatório intercalar e anual.

Os relatórios aprovados pelo Conselho Diretivo, devem posteriormente ser remetidos ao CPC e IGMTSSS, bem como ao MENAC quando aplicável.

Revisão do Plano

É efetuada uma avaliação periódica dos riscos, de periodicidade, no mínimo, anual, em função da qual poderá haver necessidade de rever ou atualizar o plano. O plano deve ser revisto sempre que se verifiquem alterações regulamentares, legislativas ou normativas aplicáveis e sempre que existam alterações significativas no contexto interno e/ou externo do Instituto de Informática.

Sempre que os responsáveis das unidades orgânicas identifiquem novos riscos e/ou alterações ao grau de risco (fora do período anual de avaliação de risco), devem identificar o mesmo, junto do Gestor do PIT, que articulará com o Responsável pela Conformidade Anticorrupção para análise e avaliação dos riscos, reunindo outros intervenientes que considerem pertinentes e necessários, podendo resultar numa revisão do plano.

B. PLANO DE PREVENÇÃO DO RISCO DE FRAUDE

1. PLANO DE PREVENÇÃO DO RISCO DE FRAUDE

No- cumprimento do Decreto-Lei n.º 29-B/2021, de 4 de maio, na sua atual redação, que estabelece o modelo de governação dos fundos europeus atribuídos a Portugal, através do PRR e conforme dispõe o Regulamento (UE) 2021/2412 (MRR), do Parlamento Europeu e do Conselho, de 12 de fevereiro de 2021 que cria o Mecanismo de Recuperação e Resiliência, na sua atual redação, compete ao Estado-Membro (EM), ao executar o mecanismo, adotar as medidas adequadas para proteger os interesses financeiros da União e assegurar que a utilização de fundos, em relação a medidas apoiadas pelo mecanismo, cumpre o direito da União e o direito nacional aplicáveis, em especial relativamente à prevenção, deteção e correção de situações de conflitos de interesses, duplo financiamento, fraude e corrupção.

Neste sentido, o Instituto procede em 2024 à elaboração do Plano de Prevenção do Risco de Fraude, adotando as medidas constantes na Orientação Técnica n.º 14/2023 (OT), proposta e aprovada pela Estrutura de Missão Recuperar Portugal.

As medidas constantes na OT, e que o Instituto adota, tem a finalidade de garantir a proteção dos interesses financeiros da União Europeia e prevenir, detetar, reportar e corrigir as situações de fraude, corrupção, conflitos de interesses e duplo financiamento, no quadro do Decreto-Lei nº 29-B/2021 de 4 de maio, na redação conferida pelo Decreto-Lei n.º 61/2023, de 24 de julho, no respeito pelo artigo 22º do Regulamento da (EU) 2021/241 do Parlamento Europeu e do Conselho, de 12 de fevereiro de 2021, que cria o Mecanismo de Recuperação e Resiliência, na sua atual redação, e das obrigações assumidas por Portugal no Contrato de Financiamento e no Contrato de Empréstimo assinados com a Comissão Europeia.

Assim o Plano de Prevenção do Risco de Fraude do Instituto identifica as situações potenciadoras do risco de fraude, elenca os controlos que minimizam a sua probabilidade de ocorrência e impacto e define o plano de ação que agrega todas as medidas de prevenção previstas, bem como os respetivos responsáveis pela sua aplicação. Define, ainda, os mecanismos de monitorização e revisão periódica do processo de gestão do risco, consubstanciando, desta forma, um instrumento de gestão fundamental e de grande utilidade para o Instituto de Informática.

Metodologia de Avaliação do Risco

A metodologia utilizada para a autoavaliação do risco de fraude, com as necessárias adaptações decorrentes das especificidades da atividade do Instituto de Informática, I.P., consta do documento da Comissão Europeia "*Guidance for Member States and Programme Authorities on fraud risk assessment and effective and proportionate anti-fraud measures* (EGESIF_14-0021-00, de 16/06/2014)".

O documento em causa foi disponibilizado aos Estados-Membros no âmbito dos FEEI, constituindo uma relevante ferramenta de avaliação de risco, estruturada em suporte Excel e integrando o Manual de Gestão do Risco da Recuperar Portugal, incluindo o risco de fraude, a qual assenta nas seguintes etapas metodológicas:

1. Quantificação da probabilidade e do impacto de um determinado risco de fraude (risco bruto);
2. Avaliação da eficácia dos controlos atualmente implementados na mitigação do risco bruto;
3. Avaliação do risco residual após o efeito dos controlos atuais e da sua eficácia, ou seja, a situação tal como é atualmente;
4. Avaliação do efeito dos controlos planeados no risco residual;
5. Definição do risco alvo, ou seja, do nível que o Instituto de Informática considera tolerável.

Assim, partindo dos riscos identificados em cada uma das atividades suscetíveis de comportarem riscos de fraude, através da ferramenta em causa, a equipa responsável pela avaliação do risco, identificada neste documento, procede à identificação dos mecanismos de controlo associados a cada uma das atividades de risco.

Todo o processo de avaliação é devidamente documentado, o que permitirá, sempre que necessário, uma revisão das conclusões obtidas.

O detalhe de cada etapa da metodologia enunciada encontra-se descrito abaixo.

Etapa 1 – Cálculo do Risco Bruto

O Risco Bruto é o nível de risco existente antes de se ter em conta o efeito de quaisquer controlos efetuados ou previstos. A quantificação do risco consiste normalmente numa combinação da "probabilidade" do mesmo – quão provável é de acontecer e o "impacto" do risco – que consequências terá financeira e não financeiramente.

<table>
<tr><th>Designação</th><th colspan="2">Orientações</th></tr>
<tr><td rowspan="6">Impacto do Risco (Bruto)</td><td colspan="2">A partir do menu de seleção, a equipa de avaliação deverá selecionar uma valoração de 1 a 4, de acordo com a consequência que o risco teria caso tivesse ocorrido, de acordo com os seguintes critérios:</td></tr>
<tr><td>Classificação</td><td>Por Objetivos</td></tr>
<tr><td>1 – Impacto limitado</td><td>Trabalhos adicionais atrasam outros processos</td></tr>
<tr><td>2 – Impacto reduzido</td><td>Concretização do objetivo operacional adiado</td></tr>
<tr><td>3 - Grande impacto</td><td>Concretização dos objetivos operacionais pode estar comprometida ou adiada</td></tr>
<tr><td>4 – Inquérito formal por parte dos interessados</td><td>Objetivos estratégicos comprometidos</td></tr>
<tr><td rowspan="5">Probabilidade do Risco (Bruto)</td><td colspan="2">A partir do menu de seleção, a equipa de avaliação do risco deverá selecionar uma pontuação de 1 a 4 da probabilidade do risco, baseada na probabilidade do risco ocorrer no período dos 6 anos de execução do PRR, de acordo com os seguintes critérios:</td></tr>
<tr><td colspan="2">Classificação</td></tr>
<tr><td colspan="2">1 – Quase nunca ocorrerá</td></tr>
<tr><td colspan="2">2 – Raramente ocorrerá</td></tr>
<tr><td colspan="2">3 – Ocorrerá algumas vezes</td></tr>
<tr><td rowspan="5">Classificação Total do Risco (Bruto)</td><td colspan="2">Este campo é automaticamente calculado a partir das informações de Impacto e Probabilidade do Risco. É classificado de acordo com a seguinte pontuação:</td></tr>
<tr><td colspan="2">Pontuação</td></tr>
<tr><td colspan="2">1 – 3 Tolerável (verde)</td></tr>
<tr><td colspan="2">4 – 6 Significante (Laranja)</td></tr>
<tr><td colspan="2">8 – 16 Crítico (Vermelho)</td></tr>
</table>

Etapa 2 – Controlos de Mitigação do Risco

Na ferramenta de autoavaliação encontra-se pré-definido um conjunto de controlos, não obstante podem ainda ser adicionados outros que se considerem adequados para mitigar os riscos identificados.

Poderá acontecer que um controlo atualmente atribuído a um risco particular, também possa ser relevante para outros riscos - em tais casos, os controlos podem ser repetidos tantas vezes quanto as necessárias.

Designação	Orientações
Refª Controlo	Uma única referência de controlo. Os números foram sequencialmente atribuídos a cada risco. Este campo apenas necessita de ser preenchido para os novos riscos identificados.
Descrição do Controlo	Este campo apenas necessita de ser preenchido para os novos riscos identificados.
Qual a fonte de informação que prevê a execução deste controlo?	Deverá ser identificado a fonte de informação em que se encontra prevista a execução do controlo, por exemplo em determinada atividade de algum Processo da Cadeia de Valor ou no Manual de Controlo Interno, etc
Existe evidência da operacionalização deste controlo?	A partir do menu de seleção a equipa de avaliação de riscos deverá selecionar "sim" ou "não" se a evidência do controlo se encontra documentada.
O controlo é regularmente testado?	A partir do menu de seleção, a equipa de avaliação de riscos deverá selecionar "sim" ou "não" para confirmar se a operacionalização do controlo é testada com regularidade. Esta tarefa poderá ser avaliada por uma equipa de auditoria interna ou externa, ou por qualquer outro mecanismo de monitorização.
Qual o nível de confiança relativamente à eficácia deste controlo?	Com base nas respostas às duas anteriores questões, a equipa de avaliação de riscos deverá indicar qual o nível de confiança relativamente à eficácia do controlo na mitigação dos riscos identificados (alta, media ou baixa). Se a eficácia do controlo não é clara ou não é testável, o nível de confiança será baixo. Se o controlo não é evidente, então claramente, não será testável.
Resultado do efeito de controlos combinados no impacto de risco, considerando os níveis de confiança	A partir do menu de seleção, a equipa de avaliação de riscos deverá indicar uma pontuação de -1 a -4, valorando o quanto se acredita que o impacto do risco foi reduzido pelos controlos existentes. Os controlos que detetam fraudes reduzem o impacto dessa fraude se demonstrarem que o mecanismo de controlo interno funciona.
Resultado do efeito dos controlos combinados na probabilidade de riscos, tendo em conta os níveis de confiança	A partir do menu de seleção, a equipa de avaliação de riscos deverá indicar uma pontuação de -1 a -4, indicando o quanto se acredita que a probabilidade de ocorrência do risco terá sido reduzida pelos controlos existentes. Os controlos que detetam fraudes reduzindo o impacto da fraude apenas reduzem de forma indireta a probabilidade de ocorrência de fraudes.

Etapa 3 – Apuramento do Risco Residual

O Risco Residual é o nível de risco após ter em consideração o efeito da realização de qualquer controlo e a sua eficácia, ou seja, a situação tal como é na realidade.

Designação	Orientações
Impacto do Risco (Residual)	Esta célula é automaticamente calculada através da dedução do efeito combinado dos controlos que mitigam o Impacto do Risco Bruto. O resultado deve ser revisto tendo em conta os seguintes critérios de forma a confirmar se a avaliação se mantém razoável:

	Classificação	Por Objetivos
	1 – Impacto limitado	Trabalhos adicionais atrasam outros processos
	2 – Impacto reduzido	Concretização do objetivo operacional adiado
	3 - Grande impacto	Concretização dos objetivos operacionais pode estar comprometida ou adiada
	4 – Inquérito formal por parte dos interessados	Objetivos estratégicos comprometidos
Probabilidade do Risco (Residual)	Esta célula é automaticamente calculada através da dedução do efeito combinado dos controlos que mitigam a Probabilidade do Risco Bruto. O resultado deve ser revisto com base nos seguintes critérios para confirmar a razoabilidade da avaliação:	
	Classificação	
	1 – Quase nunca ocorrerá	
	2 – Raramente ocorrerá	
	3 – Ocorrerá algumas vezes	
	4 – Ocorrerá com frequência	
Classificação Total do Risco (Residual)	Esta célula é automaticamente calculada através dos valores do Impacto do Risco e da Probabilidade. Será classificada de acordo com os seguintes intervalos:	
	Pontuação	
	1 – 3 Tolerável (verde)	
	4 – 6 Significante (Laranja)	
	8 – 16 Crítico (Vermelho)	

Etapa 4 – Plano de Ação para a Concretização de Medidas Antifraude Eficazes

Quando o Risco Residual permanece a um nível superior ao "tolerável" torna-se necessária a implementação de controlos adicionais que permitam contribuir para atenuar o Risco Residual, o qual ainda não foi tratado de forma eficaz pelos controlos atuais. Para o efeito devem ser identificados na ferramenta de autoavaliação os seguintes elementos:

Designação	Orientações
Controlo adicional planeado	Deve ser apresentada uma descrição completa dos controlos planeados/medidas antifraude eficazes e proporcionadas
Responsável	Deverá ser identificado um responsável, que pode ser individual ou por área funcional, para qualquer controlo planeado. Este responsável deve concordar em

	assumir a responsabilidade pelo controlo nomeadamente na sua implementação e funcionamento efetivo.
Prazo de implementação	Deve ser apresentado um prazo para a implementação do novo controlo.
Resultado do efeito combinado dos controlos adicionais no impacto do risco residual	A partir do menu de seleção a equipa de avaliação do risco deve selecionar uma pontuação entre -1 a -4 refletindo o quanto acredita que o impacto do risco será reduzido através dos novos controlos planeados.
Resultado do efeito combinado dos controlos adicionais na probabilidade do risco residual	A partir do menu de seleção a equipa de avaliação do risco deve selecionar uma pontuação entre -1 a -4 refletindo o quanto acredita que a probabilidade do risco será reduzida através dos novos controlos planeados.

Etapa 5 – Apuramento do Risco Alvo

O Risco Alvo é o nível de risco após ter em consideração o efeito de todos os controlos, atuais e adicionais planeados.

Designação	Orientações	
Impacto do Risco (Alvo)	Esta célula é automaticamente calculada através da dedução do efeito combinado dos controlos que mitigam o Impacto do Risco Residual. O resultado deve ser revisto tendo em conta os seguintes critérios de forma a confirmar se a avaliação se mantém razoável:	
	Classificação	Por Objetivos
	1 – Impacto limitado	Trabalhos adicionais atrasam outros processos
	2 – Impacto reduzido	Concretização do objetivo operacional adiado
	3 - Grande impacto	Concretização dos objetivos operacionais pode estar comprometida ou adiada
	4 – Inquérito formal por parte dos interessados	Objetivos estratégicos comprometidos
Probabilidade do Risco (Alvo)	Esta célula é automaticamente calculada através da dedução do efeito combinado dos controlos que mitigam a Probabilidade do Risco Residual. O resultado deve ser revisto com base nos seguintes critérios para confirmar a razoabilidade da avaliação:	
	Classificação	
	1 – Quase nunca ocorrerá	
	2 – Raramente ocorrerá	
	3 – Ocorrerá algumas vezes	

	4 – Ocorrerá com frequência
Pontuação Total do Risco (Alvo)	Esta célula é automaticamente calculada através dos valores do Impacto do Risco e da Probabilidade. Será classificada de acordo com os seguintes intervalos:
	Pontuação
	1 – 3 Tolerável (verde)
	4 – 6 Significante (Laranja)
	8 – 16 Crítico (Vermelho)

EQUIPA DE GESTÂO DO RISCO

A responsabilidade geral pela gestão do risco, constitui atribuição da Equipa Multidisciplinar abaixo indicada, participando nessa avaliação representantes dos seguintes departamentos:

Nome Departamento	Nome Interlocutor
Departamento Gestão Serviços e Relações Externas	Joana Vallera
Departamento Administração Sistemas	Carlos Amado
Departamento de Arquitetura e Desenvolvimento	Paulo Antunes
Departamento de Gestão Aplicações	Sofia Pedroso
Departamento de Gestão de Informação	Pedro Rodrigues
Departamento de Organização e Gestão Pessoas	Helga Beirão
Departamento de Apoio ao Utilizador	Sérgio Duarte

A Responsável por esta Equipa será a Diretora do Departamento Gestão Serviços e Relações Externas, Joana Vallera.

Ao Responsável da Equipa cabe, reunir com todos os elementos e garantir que a avaliação do risco de fraude é realizada de acordo com a metodologia e instrumentos adotados e na periodicidade definida.

Esta Equipa é Responsável por:

- Identificar os Riscos
- Identificar os Controlos existentes e aplicáveis aos Riscos
- Avaliar os Riscos (impacto e probabilidade)
- Classificar os Riscos
- Identificar a Estratégia de ação
- Definir as ações a Implementar e identificar os seus responsáveis

A Área de Qualidade e Auditoria, participará nestas avaliações na qualidade de:

- Observador – Célia de Vasconcelos
- Facilitador do Processo – Edite Estopa, Responsável Processo Gestão do Risco

Garantindo a monitorização das Ações Corretivas e de Melhoria, de acordo com o descrito no procedimento existente, e a Elaboração dos Relatórios de Acompanhamento/Avaliação, exigíveis ao abrigo da Orientação Técnica em referência.

C. CÓDIGO DE ÉTICA E CONDUTA DO INSTITUTO

CAPÍTULO I

ÂMBITO DE APLICAÇÃO E OBJETIVOS

Artigo 1.º
Âmbito

1. Este código aplica-se a todos os Trabalhadores do Instituto de Informática, I.P., doravante, Trabalhadores, independentemente da natureza do vínculo ou posição hierárquica que ocupem.
2. O presente instrumento é complementar da promoção dos valores inerentes à integridade profissional, não impede a aplicação simultânea das regras de conduta específicas de grupos profissionais, bem como as normas que integram o Exercício do Poder Disciplinar dos Trabalhadores que exercem Funções Públicas e a Carta Ética da Administração Pública.

Artigo 2.º
Princípios Gerais

1. O presente Código de Ética e de Conduta pretende constituir uma das bases para a qualidade da intervenção do Instituto de Informática, I.P., integrando um conjunto de princípios éticos e de normas de conduta para todos os seus Trabalhadores, a observar no desempenho das suas funções profissionais, contribuindo para a afirmação de uma imagem institucional de rigor, eficiência, competência, confiança, compromisso e inovação.
2. Os Trabalhadores devem promover e incentivar a adoção dos princípios de atuação e das regras de conduta definidas no que respeita às relações entre si, com os fornecedores, com os parceiros institucionais e com os cidadãos e agentes económicos.
3. No exercício das suas funções, os Trabalhadores do Instituto de Informática, I.P. estão exclusivamente afetos ao serviço do interesse público.
4. Os Trabalhadores, devem ainda, observar os valores fundamentais e os princípios da atividade administrativa, designadamente os da legalidade, imparcialidade, competência, responsabilidade e transparência de forma a assegurar a integridade, a independência, a credibilidade e a eficácia no exercício das competências que lhes estão cometidas.

CAPÍTULO II
NORMAS DE CONDUTA

Artigo 3.º
Prossecução do Interesse Público e Isenção

1. Os Trabalhadores devem nortear toda a sua atuação no sentido de prosseguir o interesse público, com respeito pela Constituição, e pelas leis, bem como pelos direitos e interesses legalmente protegidos dos cidadãos.
2. Os Trabalhadores devem atuar com isenção, em relação a todos aqueles com os quais tenham ou venham a ter qualquer tipo de relacionamento na sua atividade profissional.

Artigo 4.º

Imparcialidade

Os Trabalhadores devem agir com imparcialidade, desempenhando as suas funções com equidistância a todas as entidades e pessoas com quem estabeleçam uma relação em virtude do exercício das suas funções, sem discriminar positiva ou negativamente qualquer deles, na perspetiva do respeito pela igualdade dos cidadãos.

Artigo 5.º
Autonomia

Consoante as funções desempenhadas, os Trabalhadores gozam de autonomia técnica ou deontológica.

Artigo 6.º
Igualdade, Diversidade e Não Discriminação

1. O Instituto de Informática, I.P. compromete-se a respeitar os princípios da igualdade e da diversidade, cumprindo a legislação nacional e internacional, e a não admitir qualquer forma de discriminação individual, que seja incompatível com a dignidade da pessoa humana, nomeadamente, em razão do género, origem, etnia, confissão política e/ou cultural e/ou religiosa, orientação sexual ou deficiência e condena qualquer forma de coerção física ou verbal, incluindo assédio moral e sexual.
2. O Instituto de Informática, I.P. promove políticas e medidas destinadas a prevenir atuações discriminatórias, sensibilizando para a diversidade, a inclusão e a igualdade de oportunidades.
3. Em matéria de igualdade de género, o Instituto de Informática, I.P. garante uma efetiva igualdade de tratamento e de oportunidades entre homens e mulheres, eliminando as discriminações, facilitando a conciliação da vida pessoal, familiar e profissional e adotando medidas que conduzam ao objetivo da presença plural de mulheres e de homens nos cargos de direção.
4. O direito à reserva da intimidade da vida privada deve ser escrupulosamente respeitado.

Artigo 7.º
Sustentabilidade

1. O Instituto de Informática, I.P., no desempenho da sua missão e em coerência com os seus valores institucionais, compromete-se a respeitar os três pilares da Sustentabilidade: Ambiental, Económico e Social.
2. O Instituto de Informática, I.P. assume a responsabilidade dos impactos das suas decisões e atividades, promovendo um comportamento ético e transparente que contribua para o desenvolvimento sustentável e o bem-estar da sociedade.
3. Para isso, os Trabalhadores devem ter uma participação ativa nas políticas de preservação do ambiente, gestão de resíduos e eficiência energética, bem como nas iniciativas de carácter social e solidário, promovidas pelo Instituto de Informática, I.P..

Artigo 8.º

Diligência, Eficiência, Zelo e Responsabilidade

1. A atuação dos Trabalhadores deve pautar-se pela lealdade para com o Instituto, ser honesta, imparcial, isenta e não atender a interesses pessoais.
2. Os Trabalhadores devem aderir aos mais elevados padrões de ética profissional.
3. Os Trabalhadores devem cumprir rigorosamente os horários, comparecendo sempre que solicitados, em reuniões internas ou externas.
4. Os Trabalhadores devem identificar e fornecer aos superiores hierárquicos e colegas, em tempo útil e de forma completa e rigorosa, todas as informações que possam ser relevantes para o bom andamento dos trabalhos.
5. No exercício das suas funções, os Trabalhadores devem zelar pela utilização mais eficiente, eficaz e económica dos recursos públicos, nomeadamente, executando as suas tarefas de forma diligente, praticando os atos e tomando decisões com celeridade e em tempo útil, evitando o desperdício e a dilação, devendo maximizar a qualidade dos resultados.
6. No exercício das suas funções, devem os Trabalhadores zelar pelo correto manuseamento e conservação dos equipamentos, designadamente material informático, telecomunicações e viaturas, que utilizam na prossecução da sua atividade.
7. Os Trabalhadores devem assumir a responsabilidade pelos seus atos e decisões, designadamente identificando sempre de forma clara a respetiva autoria.

Artigo 9.º

Conflito de Interesses

1. Os Trabalhadores devem evitar qualquer situação suscetível de originar, direta ou indiretamente, conflitos de interesses, cumprindo em especial as disposições legais ou contratuais, sobre garantias de imparcialidade.
2. Os Trabalhadores podem exercer atividades fora do seu horário de trabalho, sejam ou não remuneradas, desde que não interfiram com as suas obrigações profissionais, não deem origem a conflitos de interesses e se encontrem autorizadas nos termos da lei.
3. Os Trabalhadores não podem oferecer, solicitar, receber ou aceitar, para si ou para terceiros, quaisquer benefícios, dádivas e gratificações, recompensas, presentes ou ofertas, em virtude do exercício das suas funções, nos termos legalmente previstos, exceto as ofertas entregues ou recebidas por força do desempenho das funções em causa que se fundamentem numa mera relação de cortesia e que tenham valor estimado inferior a 150 euros.
4. O valor das ofertas é contabilizado no cômputo de todas as ofertas de uma pessoa, singular ou coletiva, no decurso de um ano civil.
5. A aceitação de bens de valor estimado igual ou superior a 150 euros, que constituam ou possam ser interpretadas, pela sua recusa, como uma quebra de respeito interinstitucional, devem ser aceites em nome do Instituto de Informática, I.P., e entregues ao Secretário do Conselho Diretivo, que delas mantém um registo de acesso público.
6. Os trabalhadores que, no exercício das suas funções, esteja perante uma situação passível de configurar um conflito de interesses, devem subscrever declaração individualizada de conflito de interesses, declarando-se impedidos e solicitando escusa do desempenho das funções atribuídas na sua atividade, comprometendo-se a comunicar, de imediato, ao seu superior hierárquico.

Artigo 10.º

Corrupção e Infrações Conexas

1. A atividade do Instituto de Informática, I.P. está sujeita a rigorosos mecanismos de controlo interno e externo, a normas orientadores, bem como o Plano de Prevenção de Riscos de Corrupção e Infrações Conexas.

2. Os Trabalhadores devem proceder de acordo com critérios de razoabilidade e prudência, devendo informar o superior hierárquico, ou em função da natureza envolvida, outras entidades, designadamente Ministério Público, Tribunal de Contas- ou OLAF, sempre que tomem conhecimento ou tiverem suspeitas fundadas da ocorrência de atividades de abuso de informação privilegiada, corrupção ou infrações conexas.

Artigo 11.º

Sigilo Profissional e Proteção de Dados

1. Os Trabalhadores, durante o exercício das suas funções, ou após a suspensão ou cessação das mesmas, ficam sujeitos ao sigilo profissional, relativamente a informação sobre dados pessoais ou da atividade do Instituto de Informática, I.P., salvo quando essa informação estiver licitamente no domínio público.

2. A utilização da informação do Instituto de Informática, I.P. está sujeita a regras constantes do Regulamento de Utilização de Informação.

3. O Instituto de Informática, I.P. respeita criteriosamente as normas legais e as orientações das autoridades competentes em matéria de proteção de dados pessoais, designadamente sobre a existência e alteração de ficheiros, direitos de consulta e correção dos dados pessoais neles contidos.

Artigo 12.º

Segurança de Sistemas de Informação

1. A segurança dos sistemas de informação do Instituto de Informática, I.P. tem como objetivo proteger a continuidade do serviço público, minimizando o risco de danos, prevenindo os incidentes e reduzindo o seu potencial impacto.

2. Os Trabalhadores devem observar escrupulosamente as normas de segurança do sistema de informação.

Artigo 13.º

Relações com Fornecedores

A aquisição de bens e serviços pelo Instituto de Informática, I.P. pauta-se por princípios de eficácia, eficiência e economia, sendo assegurada a transparência e a equidade no relacionamento com os diversos fornecedores.

CAPÍTULO III
DISPOSIÇÕES FINAIS

Artigo 14.º

Dever de Comunicação

1. Os Trabalhadores têm a responsabilidade de se manifestarem, ao presenciarem ou suspeitarem de condutas inadequadas.
2. O Instituto de Informática analisará atentamente cada caso de forma mais confidencial possível, tomando medidas imediatas e apropriadas relativamente a condutas inapropriadas.
3. Caso os Trabalhadores se deparem com questão legal ou ética, e não encontrem resposta no presente código devem obter aconselhamento junto do superior hierárquico ou do Gestor do Plano de Integridade e Transparência.
4. O Instituto de Informática, I.P. deve proteger os Trabalhadores que de boa-fé apresentem uma denúncia ou dúvida sobre condutas inapropriadas.

Artigo 15.º
Relacionamento com a Comunicação Social

Em matéria que se relacione com a atividade do Instituto de Informática, I.P., os Trabalhadores somente podem conceder entrevistas ou prestar informações que não sejam do domínio público, seja por iniciativa própria, seja a pedido dos meios de comunicação social, quando tenham sido autorizados por escrito para esse efeito pela Presidente do Instituto de Informática.

Artigo 16.º
Acumulação de Funções

1. Os Trabalhadores podem acumular funções ou atividades nos termos legalmente estabelecidos e devidamente autorizadas, dependendo de comunicação escrita ao superior hierárquico, para análise e verificação de incompatibilidades.
2. Os Trabalhadores que se encontram em regime de acumulações de funções devem, assim, declarar por escrito, aos respetivos superiores hierárquicos, que as atividades que desenvolvem não colidem sob forma alguma com as funções públicas que desempenham no Instituto, nem colocam em causa a isenção e o rigor que pautam a sua atuação.

Artigo 17.º
Formação

Os trabalhadores têm o dever de frequentar os cursos anuais de *e-learning* que versem sobre os conteúdos do Plano de Integridade e Transparência.

Artigo 18.º
Poder Disciplinar

Os Trabalhadores que não cumpram o estabelecido neste Código estão sujeitos a ação disciplinar, nos termos legalmente aplicáveis.

Artigo 19.º
Publicitação e Entrada em Vigor

1. O Código de Ética e de Conduta é publicitado na *intranet e no* site institucional[2] do Instituto de Informática, I.P., sendo entregue a cada Trabalhador um exemplar.
2. O presente Código de Ética e de Conduta entra em vigor no dia seguinte ao da publicitação no site institucional do Instituto de Informática, I.P..

[2] Veja-se site institucional, *in http://www.seg-social.pt/ii-ip-instituto-de-informatica-ip*

D. REGULAMENTO DE UTILIZAÇÃO DE INFORMAÇÃO

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º
Objeto e âmbito de aplicação

1. O presente regulamento define as regras e princípios para a utilização de informação no Instituto de Informática, I.P., de acordo com a legislação em vigor.
2. O Instituto de Informática, I.P. é detentor de elementos tecnológicos de base e de informação necessária à prossecução das atribuições do Ministério do Trabalho, Solidariedade e Segurança Social, assumindo a obrigação de manter a disponibilidade, confidencialidade, e integridade da mesma, bem como a privacidade dos dados pessoais materializado no Sistema de Gestão de Segurança de Informação.
3. O Instituto de Informática, I.P. é detentor de múltiplos direitos sobre produtos que resultam de investigação e desenvolvimento, pretendendo salvaguardar a confidencialidade dos mesmos.
4. O Instituto de Informática, I.P. é proprietário e detentor de bases de dados que se enquadram na sua atividade.
5. O Regulamento de Utilização de Informação aplica-se a todo o pessoal, a exercer funções no Instituto de Informática, I.P., independentemente do regime jurídico, posição hierárquica que ocupem e da natureza das suas funções.
6. O Regulamento aplica-se, ainda, a colaboradores externos que, temporariamente prestem serviços no Instituto de Informática, I.P..
7. Os trabalhadores e colaboradores externos serão doravante designados por Utilizadores.
8. O Utilizador poderá contactar o Encarregado de Proteção de Dados no sentido de obter esclarecimentos sobre a garantia da privacidade dos seus dados, ou exercício dos seus direitos ao abrigo do Regulamento Geral de Proteção de Dados.

Artigo 2.º
Definições

Para o proposto neste regulamento considera-se:

a) Informação Pública, a informação que o Instituto disponibiliza livremente a terceiros.
b) Informação de Uso Interno, a informação que se destina única e exclusivamente a uso interno.
c) Informação Confidencial, a informação que só pode ser partilhada com Utilizadores devidamente autorizados na medida do necessário.

Artigo 3.º
Ética e Conduta Profissional

1. O Utilizador deve partir do princípio de que todas as informações no local de trabalho são confidenciais, exceto quando tiver conhecimento explícito do contrário.
2. Incumbe ao Utilizador não fornecer informações confidenciais aos demais Utilizadores se não tiverem necessidade das mesmas.

3. Ao Utilizador é exigido que nunca aceda a sistemas ou utilize informações internas ou confidenciais, exceto por motivos relacionados com o seu próprio trabalho.
4. Se o Utilizador tiver conhecimento ou suspeitar que alguém tem acesso à sua palavra-passe, deve alterá-la imediatamente.
5. O Utilizador deve evitar analisar ou discutir dados confidenciais em locais onde uma pessoa não autorizada possa ver ou ouvi-los.
6. Antes de o Utilizador partilhar informações não destinadas ao público, de uso interno ou confidenciais, com parceiros de negócios externos, confirme junto do seu dirigente se é necessário implementar um acordo de não divulgação.
7. O Utilizador deve tomar precauções para proteger as informações a que tenha acesso, assim como proteger ficheiros e dispositivos de armazenamento e bloquear o seu computador de trabalho.
8. Ao Utilizador é exigido o sentido de responsabilidade na utilização da informação disponibilizada internamente, devendo adotar sempre um comportamento adequado para com a Instituição, os seus colegas de trabalho e a atividade profissional desenvolvida.
9. O Utilizador deve sempre salvaguardar a boa imagem e prestígio do Instituto de Informática, I.P..
10. O Utilizador deve ter conhecimento das políticas de segurança da informação em vigor no Instituto de Informática, I.P..
11. Caso o Utilizador venha a tomar conhecimento de uma possível violação da privacidade da informação à responsabilidade do Instituto de Informática, I.P., deve registar de imediato o incidente correspondente pelo procedimento em vigor, informando o seu superior hierárquico.
12. Todos os Utilizadores, mesmo após cessação de funções no Instituto de Informática, I.P., estão sujeitos ao dever de confidencialidade e sigilo profissional.

CAPÍTULO II
DEVER DE SIGILO

Artigo 4.º
Sigilo Profissional

1. O Utilizador não pode divulgar nem fazer uso, por qualquer meio, de informação de uso interno ou confidencial a que venha a ter acesso no decurso da sua colaboração no Instituto de Informática, I.P., salvo e na medida em que seja necessário para o exercício das suas funções, cumprindo o dever de sigilo que subsistirá mesmo após a cessação de funções no referido instituto.
2. O Utilizador deve manter a confidencialidade e respeitar os direitos de natureza intelectual sobre os produtos que resultem, designadamente, da investigação e desenvolvimento, propriedade do Instituto de Informática, I.P., ou que sejam por este detido.
3. Incumbe ao Utilizador não fazer cópias pessoais de informação que pertença ou seja gerida pelo Instituto de Informática, I.P., salvo se para tal for dada autorização escrita pelo Conselho Diretivo.
4. Incumbe ao Utilizador não fazer cópias de suportes magnéticos ou de manuais de produtos de software que pertençam ou que tenham sido facultados pelo Instituto de Informática, I.P., salvo se para tal for dada autorização escrita pelo Conselho Diretivo.

Artigo 5.º
Relacionamento com Terceiros

1. No âmbito do relacionamento com terceiros (fornecedores, cidadãos e parceiros institucionais), o Utilizador deve observar as medidas necessárias para proteger a confidencialidade dos dados de natureza pessoal, técnica, económica ou financeira a que tenha ou venha a ter acesso e que possam vir a ser conhecidos por aqueles terceiros.
2. Ao Utilizador é exigida a confidencialidade sobre todos os dados disponibilizados pelo Instituto de Informática, I.P., ou por entidades terceiras, bem como sobre as informações de carácter pessoal ou processual dos beneficiários ou contribuintes da Segurança Social.
3. Incumbe ao Utilizador remover e destruir, logo que deixe de ser necessário e de acordo com os procedimentos de destruição da informação em vigor, todo e qualquer tipo de registo, qualquer que seja o suporte, relacionado com os dados analisados, salvo se for classificado como Público.
4. O Utilizador deve guardar sigilo quanto ao conteúdo das bases de dados ao cuidado do Instituto de Informática, I.P..

CAPÍTULO III
DISPOSIÇÕES FINAIS

Artigo 6.º
Infrações

1. O incumprimento das regras estabelecidas no presente Regulamento, faz o Utilizador com vínculo público incorrer em responsabilidade disciplinar prevista, designadamente nos artigos 186.º a 188.º e alíneas j) e n) do nº 3 do artigo 297º da LTFP.
2. Aos demais Utilizadores serão acionadas as respetivas cláusulas contratuais.

Artigo 7.º
Formação

Os Trabalhadores do Instituto de Informática, I.P. têm o dever de frequentar os cursos anuais de *e-learning* que versem sobre os conteúdos do Plano de Integridade e Transparência e Segurança da Informação.

Artigo 8.º
Publicitação

O presente Regulamento é publicitado na *intranet* e no site institucional[3] do Instituto de Informática, I.P..

Artigo 9.º
Entrada em Vigor

O presente regulamento entra em vigor imediatamente após a sua aprovação pelo Conselho Diretivo e publicitação no site institucional do Instituto de Informática, I.P..

[3] Veja-se site institucional, *in http://www.seg-social.pt/ii-ip-instituto-de-informatica-ip*

E. REGULAMENTO DE UTILIZAÇÃO DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

CAPÍTULO I
ÂMBITO DE APLICAÇÃO E OBJETIVOS

Artigo 1.º
Âmbito de Aplicação

1. O presente regulamento define as regras de conduta e princípios para a utilização das tecnologias de informação e comunicação no Instituto de Informática, I.P., de acordo com a legislação em vigor.
2. O Regulamento de Utilização de Tecnologias de Informação e Comunicação aplica-se a todos os trabalhadores em funções públicas, bem como colaboradores externos que, temporariamente, prestem serviço no Instituto de Informática, I.P., doravante designado(s) por Utilizador(es).

Artigo 2.º
Ética e Conduta Profissional

1. Incumbe a todos os Utilizadores assegurar o correto uso dos meios informáticos colocados à sua disposição, devendo, por regra, ser utilizados unicamente para fins profissionais.
2. Os Utilizadores devem pautar o seu comportamento pelo sentido de responsabilidade na utilização dos sistemas de informação e comunicação disponibilizados internamente, bem como os que se encontram acessíveis através de redes públicas tais como redes sociais ou plataformas semelhantes.
3. Os Utilizadores devem, ainda, adotar um comportamento adequado para com o Instituto de Informática, I.P., e seus colegas de trabalho, no quadro da atividade profissional desenvolvida.
4. Os Utilizadores devem salvaguardar a boa imagem e o prestígio do Instituto de Informática, I.P..

Artigo 3.º
Definições

No presente regulamento, entende-se nas aceções a seguir indicadas:

a) *Posto de Trabalho,* é constituído por computador, fixo ou portátil, pré-instalado com Estação Padrão (EP), rato, teclado, monitor e telefone (hardware ou software);

b) Estação Padrão, é uma solução de Desktop Corporativo que assegura a uniformização de Software nos postos de trabalho, garantindo que estes têm capacidade para suportar as necessidades de acesso aos sistemas de informação por parte dos Utilizadores.

CAPÍTULO II
POSTO DE TRABALHO

SECÇÃO I
Armazenamento e Utilização da Informação

Artigo 4.º
Informação Profissional

1. Toda a informação armazenada pelos Utilizadores no posto de trabalho reside em servidores, sem prejuízo do disposto no artigo 5º.
2. Além do espaço atribuído a cada utilizador nos servidores do II, é ainda atribuído a cada utilizador 1TB de armazenamento no Onedrive no Microsoft 365.
3. Toda a informação armazenada em servidores e na cloud M365 é propriedade do Instituto de Informática, I.P..
4. A informação só deve ser utilizada para os fins a que se destina, não devendo ser comunicada a terceiros, exceto com a necessária autorização ou permissão legal.

Artigo 5.º
Informação Pessoal

1. Os Utilizadores não devem utilizar o espaço dos servidores para armazenar informação de caráter pessoal.
2. Os Utilizadores devem guardar a documentação pessoal na Pasta do computador criada para esse fim (Pasta "L").
3. É da responsabilidade dos Utilizadores a gestão da pasta referida no número anterior, designadamente, a introdução e eliminação da informação e a realização de cópias de segurança.

Artigo 6.º
Eliminação de Ficheiros

1. O Instituto de Informática, I.P. reserva-se o direito de proceder à eliminação de todos os ficheiros de caracter pessoal armazenados em servidores, designadamente fotografias, músicas e filmes (JPEG, JPG, TIFF, PNG, DIV, AVI, Mp3, Mp4, MKV, entre outros).
2. A eliminação de ficheiros de natureza pessoal ou profissional está dependente de contacto prévio com o Utilizador e respetivo superior hierárquico, se necessário.
3. O Utilizador que necessite, por força das funções exercidas, de armazenar ficheiros com dimensão superior à normal, deve manifestar essa necessidade junto do serviço competente.

Artigo 7.º
Cópias de Segurança e Recuperação de Dados

1. A informação armazenada nos servidores e postos de trabalho é alvo de cópia diária de segurança, estando o Instituto de Informática, I.P. legitimado para recorrer à respetiva recuperação.
2. A pasta "L" existente nos postos de trabalho, não é alvo de cópia de segurança.
3. Os Utilizadores podem solicitar a recuperação de informação que foi alvo de cópia de segurança.

4. A recuperação da informação referida no número anterior está dependente da disponibilidade da mesma, de acordo com a política de cópia de segurança em vigor.

Artigo 8.º
Instalação de Software

1. Os Utilizadores não estão autorizados a instalar *software* na EP, com exceção daquele que é disponibilizado pelo Instituto de Informática, I.P. na *Store* da Estação Padrão em http://store.seg-social.pt.
2. Excecionalmente, poderá ser instalado outro tipo de software, pelos Administradores de Sistema, desde que previamente autorizado pelo superior hierárquico, justificando essa necessidade.

Artigo 9.º
Cessação ou Suspensão de Funções do Utilizador

1. Cabe ao Utilizador, antes da cessação ou suspensão, proceder à eliminação de toda a informação de caráter pessoal.
2. Após cessação ou suspensão, toda a informação constante nos sistemas informáticos é propriedade do Instituto de Informática, I.P..
3. Após a cessação ou durante suspensão os Utilizadores não estão autorizados a fazer uso de informação profissional do Instituto de Informática, I.P., salvo nas situações previstas no Regulamento de Utilização de Informação.
4. O perfil do utilizador interno ou externo que cesse funções será preservado pelo período de um ano.
5. No caso de suspensão de funções a informação do perfil desses utilizadores será preservada.

SECÇÃO II
Impressão

Artigo 10.º
Regras de Utilização

1. As impressoras são, por norma, configuradas em modo partilhado, para permitir a impressão por diversos Utilizadores.
2. O Utilizador deve fazer uma utilização rigorosa dos recursos disponíveis evitando a impressão de documentos, e sempre que for possível, recorrer a configurações que assegurem uma utilização económica das impressoras, nomeadamente a impressão a preto e em frente e verso.

Artigo 11.º
Documentos

1. O Utilizador que tenha acesso a documentos esquecidos numa impressora, deve entregá-los ao proprietário, se este for identificável.
2. Caso não seja identificável deverá destruir o documento, ao abrigo da política de segurança de informação.

SECÇÃO III

Comunicações de Dados, de Voz Fixa e Móvel e solução de colaboração

Artigo 12.º

Telefone Fixo

1. A cada Utilizador é associado um número de telefone da rede fixa que é parte integrante do posto de trabalho, bem como um perfil de comunicações que lhe permitirá realizar as chamadas necessárias ao bom exercício das suas funções.
2. Os perfis de utilização em funcionamento no Instituto de Informática, I.P., são os seguintes:
   a) Para Fax;
   b) Chamadas Internas;
   c) Chamadas Internas + Nacionais;
   d) Chamadas Internas + Nacionais + Móvel;
   e) Chamadas Internas + Nacionais + Móvel + Internacional.

Artigo 13.º

Utilização de Telefone Móvel

Todas as normas, regras e procedimentos para utilização de telefone móvel de uso oficial, encontram-se definidas pelo "Regulamento interno de atribuição e utilização de telefone móvel para uso oficial", disponível na *intranet* do Instituto de Informática, I.P..

Artigo 14.º

Utilização da solução de colaboração Microsoft Teams (ou outras)

A cada Utilizador é associado um endereço Teams (igual ao endereço de correio eletrónico), que lhe permitirá ter acesso a um conjunto de funcionalidades disponibilizado pela ferramenta, tais como: gestão de equipas e canais de comunicação, uso de Chat (conversas), efetuar reuniões e chamadas, diretamente com outros utilizadores do ambiente M365 e também com utilizadores externos que utilizem a mesma plataforma.

Artigo 15.º

Regras de Utilização

A utilização de telefone fixo, telefone móvel, soluções de colaboração e equipamento de banda larga, deve pautar-se sempre por critérios de razoabilidade e bom senso, nomeadamente atendendo às funções desempenhadas e às necessidades verificadas com vista ao adequado e correto desempenho das mesmas.

Artigo 16.º

Verificação

1. O Instituto de Informática, I.P. efetua a verificação das comunicações de voz fixa, móvel e dados e das soluções de colaboração.
2. Sempre que necessário procede à elaboração de relatórios, utilizando para o efeito os registos constantes nas diversas soluções ou com recurso a elementos fornecidos pelos operadores de comunicações.

3. Em conformidade com deliberação da CNPD (Comissão Nacional De Proteção de Dados), os dados alvo de tratamento serão limitados à identificação do Utilizador, à sua categoria/função, número de telefone chamado/recebido com supressão dos últimos 4 dígitos, tipo de chamada – local, regional e internacional -, duração da chamada e custo da comunicação.
4. Em situações de exceção, observados os limites de ordem legal, e mediante autorização do Conselho Diretivo, pode o Instituto de Informática, I.P. proceder à análise de utilização e faturação detalhada por Utilizador.

CAPITULO III
CORREIO ELETRÓNICO

Secção I
Princípios e Regras de Utilização

Artigo 17.º
Princípios

1. O correio eletrónico deve ser utilizado, em regra, para fins profissionais.
2. Em caso de utilização do correio eletrónico para fins privados, o Utilizador deverá fazer um uso adequado e responsável.
3. O Instituto de Informática, I.P., tem um serviço de correio eletrónico baseado num sistema misto, em que uma parte é garantida pela infraestrutura do II, e a outra é garantida pelo Microsoft 365 (M365), que é suportado na Cloud em infraestrutura da Microsoft.

Artigo 18.º
Regras de Utilização

1. As caixas de correio se forem suportadas no M365, têm por *default* um tamanho mínimo de 50 GB, ao qual acresce mais 50GB de arquivo, caso sejam suportadas na infraestruturo do II, têm por *default* um limite máximo de 15 Gb, passiveis de aumento para 25 Gb quando devidamente autorizado, pelo que os Utilizadores devem fazer uma utilização consciente das mesmas, arquivando todos as mensagens de correio eletrónico que se tornem obsoletas ou desnecessárias.
2. As mensagens recebidas que contenham ficheiros anexos suspeitos - de origem desconhecida ou não fidedigna - devem ser eliminadas sem abrir.
3. Se acidentalmente o Utilizador abrir uma mensagem com SPAM (publicidade não solicitada) não deve abrir ficheiros anexos ou Links (ligações que permitem aceder a uma página/ficheiro) e deve eliminá-la de imediato.
4. O envio de mensagens de correio eletrónico com ficheiros anexos não deve exceder os 15MB, nem deve ultrapassar 100 (cem) destinatários em simultâneo. Sempre que possível, é aconselhável usar uma ferramenta de colaboração para partilhar ficheiros grandes. O ambiente M365 do II, disponibiliza o Onedrive, que permite armazenar e partilhar ficheiros com tamanhos superiores a 15 MB.
5. Os ficheiros anexos à mensagem, que contenham versões finais de documentos e/ou que não se destinem a ser validados/alterados pelos destinatários da mensagem, devem ser enviados, por regra em formato PDF.

6. Com exceção dos casos autorizados superiormente, a divulgação de informação institucional, dirigida aos Utilizadores do Instituto de Informática, I.P., deve ser efetuada através do site institucional.
7. É obrigatório utilizar a assinatura institucional em todas as mensagens enviadas, e quando exigível a assinatura eletrónica qualificada.
8. Não é permitido o envio de qualquer mensagem de correio eletrónico que:
   a) Possa ser interpretada como um insulto ou ofensa por qualquer outro trabalhador ou entidade externa;
   b) Possa prejudicar a boa imagem ou reputação do Instituto de Informática, I.P.;
   c) Seja ilegal, obscena, pornográfica ou ofensiva;
   d) Tenha por objetivo ganhos financeiros ou materiais para proveito pessoal ou de terceiros;
   e) Seja destinado a um elevado número de Utilizadores, sem o seu consentimento ou conhecimento, fora do âmbito da atividade profissional;
   f) Contenha vírus ou outras formas geradoras de insegurança ou instabilidade informática, tais como *malware, spyware, phishing*;
   g) Seja considerada SPAM.

Secção II
Caixas Institucionais

Artigo 19.º
Regras de Criação

1. Os serviços do Instituto de Informática, I.P. devem solicitar a criação de caixas de correio eletrónico institucionais, sempre que se justifique, por questões de simplificação organizacional nos seus contactos com os demais serviços.
2. Os serviços do Instituto de Informática, I.P. devem ainda solicitar a criação de caixas de correio eletrónico institucionais para comunicação com entidades externas, de modo a evitar que as mensagens fiquem pendentes de tratamento em caixas pessoais.

Artigo 20.º
Regras de Utilização

1. As caixas de correio institucionais não têm limite de tamanho, pelo que os Utilizadores devem fazer uma utilização consciente das mesmas, arquivando todos as mensagens de correio eletrónico que se tornem obsoletas ou desnecessárias.
2. As mensagens lidas por qualquer um dos Utilizadores que tem acesso à caixa de correio institucional, ficam marcadas como “lidas”.
3. A eliminação de mensagens por parte de um Utilizador impede os restantes Utilizadores de terem acesso às mesmas.
4. Considerando que, por defeito, as respostas enviadas ficam residentes nas caixas de correio pessoais, deve cada Utilizador assegurar a transferência das mesmas para a caixa institucional.

Secção III
Acesso a Mensagens de Correio Eletrónico

Artigo 21.º
Ausência do Utilizador

1. No caso da ausência temporária do Utilizador, deve o próprio ativar o mecanismo de resposta automática "fora de escritório", e preferencialmente com a indicação do período de ausência.
2. Em caso de cessação ou suspensão de funções deve o Utilizador previamente assegurar o tratamento de mensagens de caráter profissional em coordenação com o seu superior hierárquico e a eliminação de todas as mensagens de caráter pessoal.
3. Caso não tenha sido possível o procedimento previsto no número anterior, o Instituto de Informática, I.P. está legitimado para aceder a todas mensagens de caráter profissional armazenadas na respetiva caixa de correio eletrónico, desde que acompanhados por um representante sindical.

Artigo 22.º
Acesso em Exercício de Funções

1. O Instituto de Informática, I.P. pode aceder às mensagens de correio eletrónico dos Utilizadores, caso as circunstâncias o justifiquem e nas condições expressas nos números seguintes.
2. O referido acesso é feito na presença do Utilizador visado e, de preferência, na presença de um representante dos trabalhadores.
3. O acesso deve limitar-se à visualização dos endereços dos destinatários, o assunto, a data e hora do envio, podendo o Utilizador impor limitações, especificando a existência de algumas mensagens de natureza privada e que não pretende que sejam lidas pelo Instituto de Informática, I.P..

CAPITULO IV
INTERNET

Artigo 23.º
Âmbito e Princípios

1. As regras definidas na presente secção aplicam-se a todos os meios informáticos que permitem o acesso à Internet disponibilizados pelo Instituto de Informática, I.P. ao Utilizador, nomeadamente telefone móvel, placa de banda larga e computador ou portátil.
2. Nas situações em que não seja possível a utilização de um equipamento individual para acesso à Internet deve o mesmo ser garantido com recurso a equipamentos de utilização partilhada.
3. Não é vedado o acesso à Internet para fins privados, devendo os Utilizadores fazê-lo de uma forma responsável e fora do seu horário de trabalho.
4. Os Utilizadores devem fazer uso adequado e responsável das redes sociais em que participam, designadamente não divulgando informação de caráter profissional.

Artigo 24.º
Monitorização e Controlo

1. Por questões de segurança encontram-se implementados mecanismos de monitorização e controlo dos acessos realizados pelos Utilizadores.
2. A monitorização e controlo referidos no número anterior, é efetuada de forma global, e não individualizada, com o objetivo de garantir os níveis de segurança e qualidade de serviço necessários ao bom funcionamento da rede interna da Segurança Social.
3. O grau de utilização da Internet no local de trabalho pode ser medido através de estudos estatísticos, de modo a aferir em que medida a utilização compromete as tarefas profissionais ou a produtividade dos trabalhadores.
4. Perante a verificação de acessos excessivos e desproporcionados do Utilizador, este poderá ser alertado.
5. O controlo do tempo de acesso diário e dos sítios consultados por cada Utilizador apenas será realizado em circunstâncias excecionais, nomeadamente por iniciativa do Utilizador quando, no contexto da sua advertência, aquele puser em causa os alertas recebidos e quiser conferir a realização de tais acessos.
6. O Instituto de Informática, I.P. pode restringir o acesso à Internet de determinados Utilizadores, em resultado de requerimento apresentado pelo seu superior hierárquico, e após comprovado uso excessivo e desproporcionado.
7. O Instituto de Informática, I.P. pode restringir o acesso a determinados sítios de Internet por razões de segurança e qualidade de serviço, necessários ao bom funcionamento da rede interna da Segurança Social.
8. Devem os Utilizadores informar os serviços competentes sobre quais os sitos de Internet que se encontram vedados e que sejam necessários aceder no desempenho das suas funções profissionais, de modo a que possa ser excecionado das regras de segurança implementadas.

CAPITULO V
ACESSOS

Artigo 25.º
Princípios

1. Ao Utilizador, no âmbito do exercício das suas funções, são permitidos diversos acessos a informação confidencial do Instituto de Informática, I.P..
2. Toda a informação criada pelo Utilizador torna-se confidencial e propriedade do Instituto de Informática, I.P..

Artigo 26.º
Utilização

1. A cada Utilizador é fornecido um código de utilizador e palavra-passe de acesso aos recursos informáticos do Instituto de Informática, I.P..
2. As palavra-passe fornecidas são pessoais e intransmissíveis.
3. É obrigatório que cada Utilizador assegure os seguintes procedimentos:
   a) Alterar periodicamente a palavra-passe, nomeadamente quando solicitado;
   b) Bloquear o computador sempre que se ausente do seu posto de trabalho;
   c) Terminar a Sessão no final do dia de trabalho.

CAPÍTULO VI
DISPOSIÇÕES FINAIS

Artigo 27.º
Formação

Os Trabalhadores do Instituto de Informática, I.P. têm o dever de frequentar os cursos anuais de *e-learning* que versem sobre os conteúdos do Plano de Integridade e Transparência.

Artigo 28.º
Infrações

O incumprimento das regras estabelecidas no presente Regulamento, faz o Utilizador incorrer em responsabilidade disciplinar.

Artigo 29.º
Entrada em vigor

O presente regulamento entra em vigor imediatamente após a sua aprovação pelo Conselho Diretivo e publicitação na *intranet* e no site institucional[4] do Instituto de Informática, I.P..

[4] Veja-se site institucional, *in http://www.seg-social.pt/ii-ip-instituto-de-informatica-ip*

F. CÓDIGO DE CONDUTA DE FORNECEDORES

Artigo 1.º
Aplicabilidade

O Código de Conduta de Fornecedores é aplicável aos Fornecedores do Instituto de Informática, I.P., e enquadra o comportamento legalmente devido dos respetivos empregados, agentes ou subcontratantes, doravante designados por Fornecedores, no desenrolar da sua atividade comercial.

Artigo 2.º
Cumprimento

1. Os Fornecedores têm o dever de informar prontamente o seu contacto designado do Instituto de Informática, I.P. e o Gestor do Plano de Integridade e Transparência, sempre que ocorra qualquer situação que possa ser considerada violação do presente Código de Conduta.
2. O Instituto de Informática, I.P. poderá exigir o afastamento imediato de quaisquer representantes ou empregados do Fornecedor cuja atuação seja gravemente contrária ao interesse público legalmente definido.

Artigo 3.º
Conformidade Regulamentar e Legal

1. Os Fornecedores devem conduzir a sua atividade comercial em total conformidade com as leis e normas aplicáveis no decorrer das suas relações contratuais com o e/ou em nome do Instituto de Informática, I.P. e em especial cumprir as obrigações fiscais.
2. Os Fornecedores têm de cumprir todas as leis de anticorrupção, antimonopólio e antibranqueamento de capitais aplicáveis, bem como as leis que regem o tráfico de influências, ofertas e pagamentos a representantes públicos, leis de contribuição para campanhas eleitorais, assim como outras normas relacionadas.
3. Os Fornecedores não deverão, direta ou indiretamente, oferecer ou pagar algo de valor (incluindo despesas com presentes, viagens, despesas de entretenimento e donativos para caridade) a qualquer dirigente ou trabalhador do Instituto de Informática, I.P., salvo nos estritos termos em que tal seja admitido em regulamento apropriado.

Artigo 4.º
Práticas Comerciais e Éticas

1. Na relação com o Instituto de Informática, I.P. os Fornecedores devem pautar os seus comportamentos pela observância dos valores da integridade e transparência.
2. Os Fornecedores devem ainda:
    a. No âmbito dos registos comerciais, registar e transmitir de forma honesta e precisa todas as informações comerciais;
    b. Criar, guardar e eliminar os registos comerciais em total conformidade com todos os requisitos legais e regulamentares aplicáveis;
    c. Ser honestos, diretos e verdadeiros nas comunicações com os representantes do Instituto de Informática, I.P..
    d. Apenas falar com a imprensa em nome do Instituto de Informática, I.P. caso tenham sido expressamente autorizados por escrito para tal;

e. Ter especial atenção às regras sobre garantias de imparcialidade constante na legislação aplicável, evitando situações inapropriadas reais ou aparentes ou de conflitos de interesses.

Artigo 5.º

Práticas Laborais e Direitos Humanos

1. O Instituto de Informática, I.P. espera que os seus Fornecedores partilhem o seu compromisso relativamente aos direitos humanos, à igualdade de género e à igualdade de oportunidades no trabalho.
2. Todos os Fornecedores devem ainda:
   a. Cooperar com o compromisso do Instituto de Informática, I.P. no sentido de promover uma mão-de-obra e um local de trabalho isentos de qualquer assédio e discriminação ilegal;
   b. Na medida em que as diferenças culturais são reconhecidas e respeitadas, abster-se de participar em atividades de discriminação designadamente em função da raça, cor, sexo, religião, orientação sexual e filiação política;
   c. Cumprir todas as leis e normas nacionais relativas à idade mínima para trabalhar e não utilizar trabalho infantil, bem como abster-se de apoiar qualquer prática relacionada com o tráfico de pessoas;
   d. Pagar aos seus trabalhadores a justa remuneração pelo trabalho desenvolvido.

Artigo 6.º

Saúde e Segurança

1. Os Fornecedores não devem obrigar os trabalhadores a um número excessivo de horas de trabalho diário.
2. Os Fornecedores devem ainda:
   a. Conceder aos seus trabalhadores o direito a, pelo menos, um dia de descanso por cada sete dias de trabalho.
   b. Manter os registos dos trabalhadores de acordo com as leis;
   c. Respeitar os direitos dos trabalhadores à liberdade de associação e de negociação coletiva de acordo com os requisitos legais;
   d. Garantir o cumprimento das obrigações, em matéria de Segurança e Saúde do Trabalho, proporcionando boas condições de trabalho, do ponto de vista físico e moral.

Artigo 7.º

Propriedade Intelectual e Obrigações de Confidencialidade

1. O respeito pelos direitos de propriedade intelectual é essencial nas relações estabelecidas entre fornecedores e o Instituto de Informática, I.P..
2. Os Fornecedores não devem utilizar tecnologia patenteada, reproduzir programas informáticos ou divulgar informações, em violação das normas de direito intelectual.
3. Os Fornecedores não devem transferir, utilizar ou publicar informações confidenciais, salvo permissão ou obrigação legal.
4. Os Fornecedores devem cumprir escrupulosamente as normas sobre proteção de dados pessoais, designadamente adotando mecanismos de segurança.

Artigo 8.º

Formação

Os Fornecedores devem assegurar a formação profissional adequada dos seus trabalhadores.

INSTITUTO
DE INFORMÁTICA

Instituto de Informática, I.P.- MTSSS
Av. Prof. Dr. Cavaco Silva, 17 – Taguspark
2740-120 Porto Salvo
Tel +351 21 423 00 00