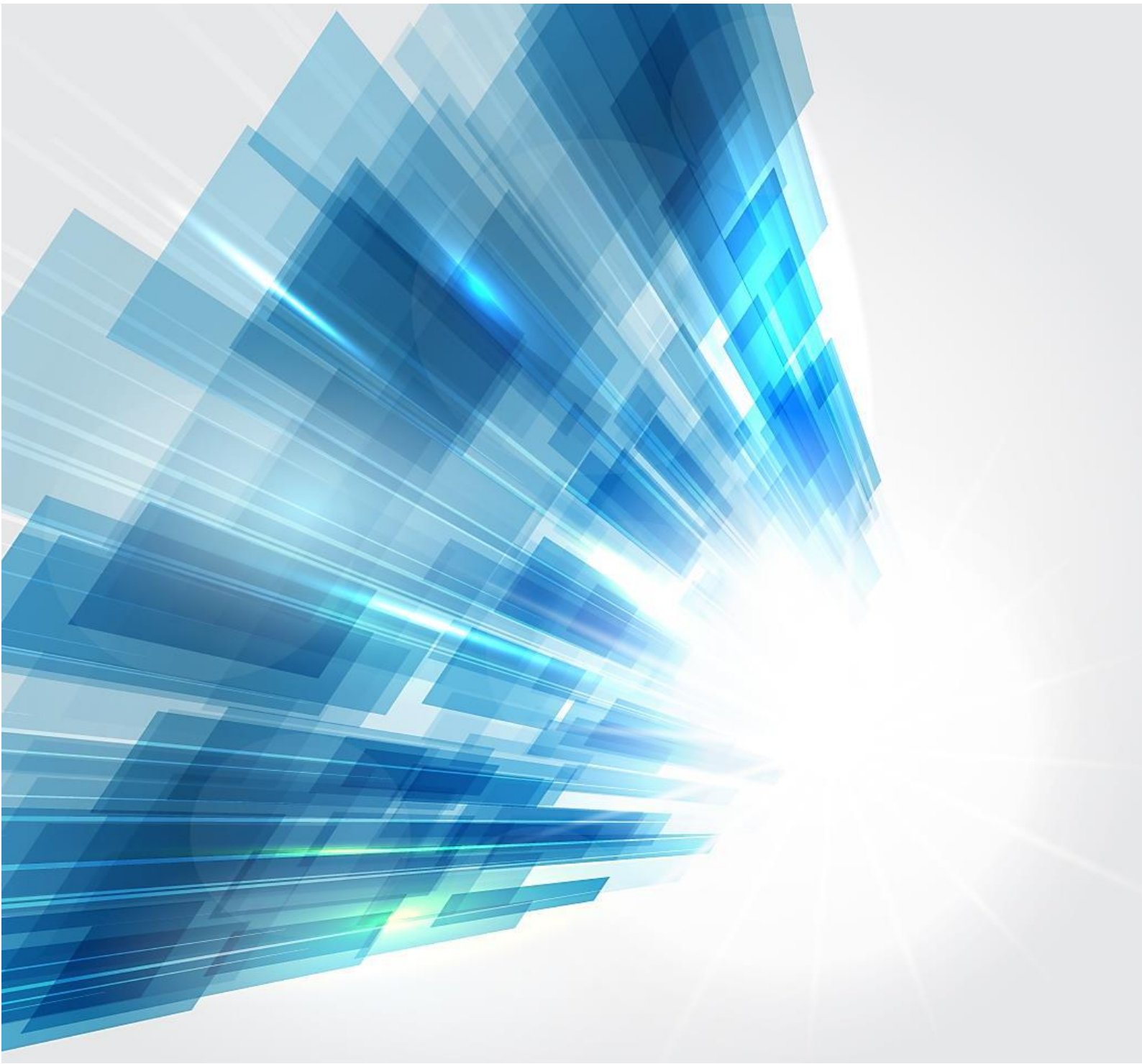
Plano de **I**ntegridade e **T**ransparência

Relatório Anual de Execução



EFQM Recognised for Excellence 3 Star - 2017

EMPRESA CERTIFICADA eiC ISO/IEC 20000-1

EMPRESA CERTIFICADA eiC ISO/IEC 27001 certificação acreditada IPAC

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.

Índice

Nota Introdutória 5

1. Estrutura Orgânica 6

1.1. Missão 6

1.2. Atribuições 6

1.3. Departamentos e Áreas Orgânicas 7

1.4. Organograma 8

2. O Plano de Integridade e Transparência 9

2.1. Enquadramento 9

2.2. Sobre o Plano 10

2.3. Responsáveis pelo Plano e respetivas funções 11

2.4. Controlo e monitorização do plano – relatórios 12

3. Execução Anual do PIT 13

3.1 Objetivos 13

3.2 Medidas de Implementação do PIT 13

3.2.1 Resultados do questionário sobre o Código de Ética e Conduta 13

3.2.2 Resultados do questionário sobre o Plano de Prevenção de Riscos de Corrupção e Infrações Conexas – Conflito de Interesses 14

3.2.3 Resultados do questionário sobre o Regulamento de Utilização de Informação 14

3.3 Medidas de redução dos riscos de corrupção e infrações conexas 15

3.4 Medidas de Prevenção ao Conluio na Contratação Pública 21

4. Conclusões 22

Histórico de Alterações

Data	Versão	Descrição	Autor(es)
05-12-2018	0.0	Redação inicial	Miguel Dias Esperança

Lista de Distribuição

Destinatário (s)	Organização
Conselho Diretivo	Instituto de Informática, I.P.
Trabalhadores	Instituto de Informática, I.P.
	Conselho de Prevenção da Corrupção
Inspetor-Geral	IGMTSSS

Nota Introdutória

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

O 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;
- 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 presente relatório tem como objetivo expor os resultados anuais da aferição da efetividade, utilidade, eficácia e correção das medidas propostas no Plano de Integridade e Transparência, doravante designado por PIT.

Apesar das medidas propostas no PIT incidirem na sua maioria na Prevenção de Riscos de Corrupção e Infrações conexas, é de realçar que se alargou o escopo para uma Gestão de Riscos, monitorizando os restantes instrumentos do PIT.

Assim, serão examinadas as operações, atividades e sistemas considerados no Plano, no período de janeiro a dezembro de 2018, com vista a verificar a percentagem de execução, os constrangimentos e as propostas de melhoria das medidas que decorreram neste período.

1. Estrutura Orgânica

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.

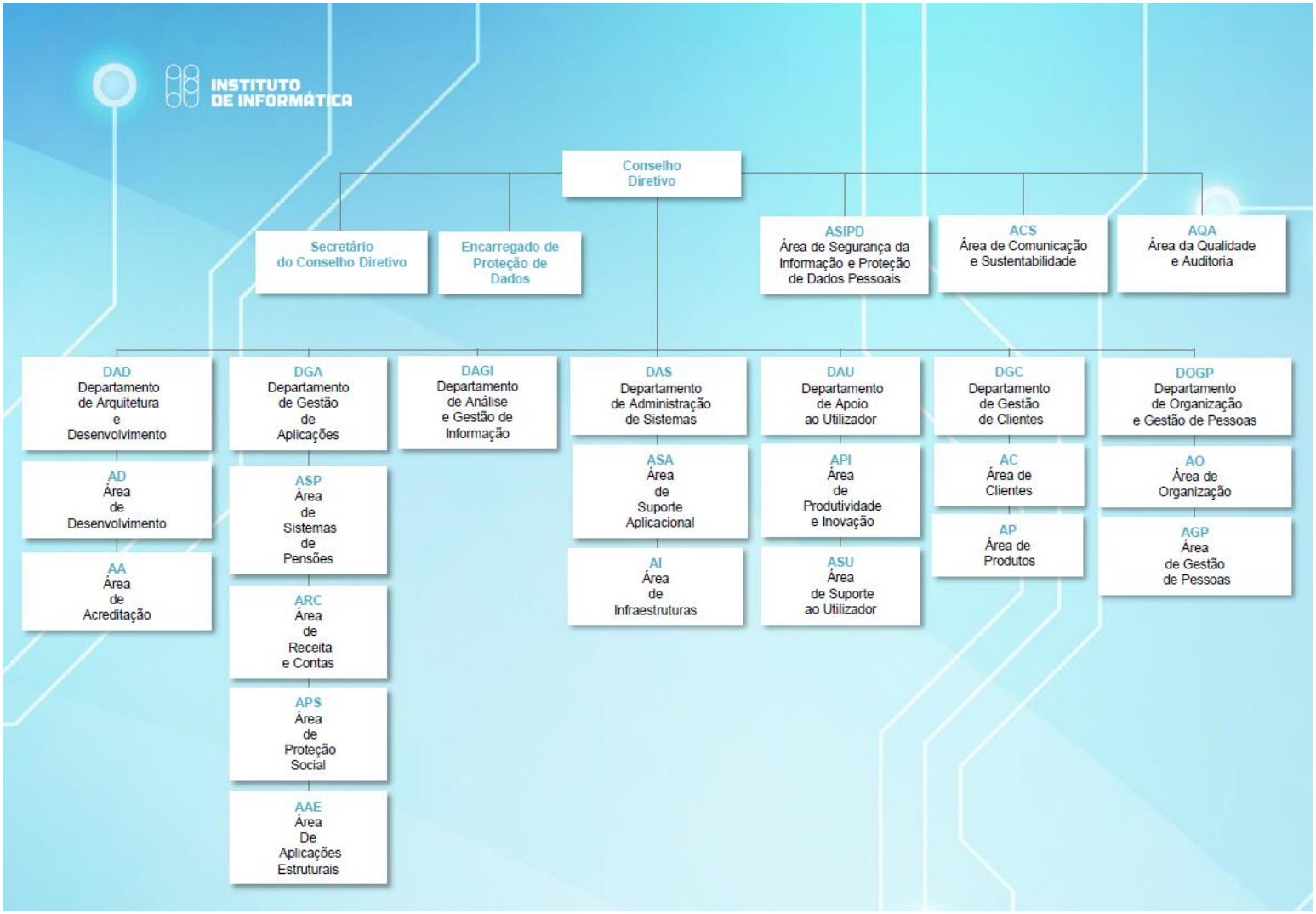
1.3. Departamentos e Áreas Orgânicas

A organização interna dos serviços do Instituto de Informática, I.P., *cfr.* Portaria n.º 138/2013, de 2 de abril, 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 Clientes;
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.

1.4. Organograma



2. O Plano de Integridade e Transparência

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 Republica, 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 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).

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.

Neste sentido, procedeu-se, à revisão do Plano de Prevenção de Riscos de Corrupção e Infrações Conexas ([1]), com a aprovação do PIT em 12 de Agosto de 2016, adaptando-o ao quadro normativo vigente e à estrutura orgânica prevista na Portaria n.º 138/2013, de 2 de abril.

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 Republica, II Serie, nº 140, de 22 de julho do Conselho de Prevenção da Corrupção, pretende-se 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 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.

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 pela Lei 67/98, de 26 de outubro, 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) dispões 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

[1] Plano de Gestão de Riscos de Corrupção e Infrações Conexas 2010-2011.

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.

2.3. Responsáveis pelo Plano e respetivas funções

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

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..

INTERVENIENTES	FUNÇÕES E RESPONSABILIDADES
Conselho Diretivo	• Compete-lhe aprovar o Plano e acompanhar a sua execução.
Gestor do Plano	• Faz a gestão do Plano. • Estabelece a arquitetura e os critérios da gestão do risco, cuidando da sua revisão quando necessário. • Acompanha a execução das medidas previstas no Plano. • Contribui para a melhoria contínua da gestão de riscos. • Elabora os respetivos Relatórios trimestrais e anuais. • Apoia na consolidação da revisão e atualização do Plano sempre que necessário.
Diretores de Departamento e Coordenadores de Área	• São os responsáveis pela organização, aplicação, e acompanhamento do Plano na parte respetiva. • Identificam, recolhem e comunicam ao Gestor, qualquer ocorrência de risco com provável gravidade maior. • Responsabilizam-se pela eficácia das medidas de controlo do risco na sua esfera de atuação.

2.4. Controlo e monitorização do plano – relatórios

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.

O Instituto de Informática, I.P. assume a responsabilidade da materialização das medidas preconizadas através da monitorização com uma periodicidade semestral, onde se faz o ponto de situação sobre as ações a implementar ou já implementadas e em execução.

3. Execução Anual do PIT

3.1 Objetivos

O presente relatório tem por base os relatórios trimestrais de execução e as 69 medidas constantes no Plano de Integridade e Transparência, expondo os resultados anuais, com vista a verificar a percentagem de execução, os constrangimentos e as propostas de beneficiação das medidas.

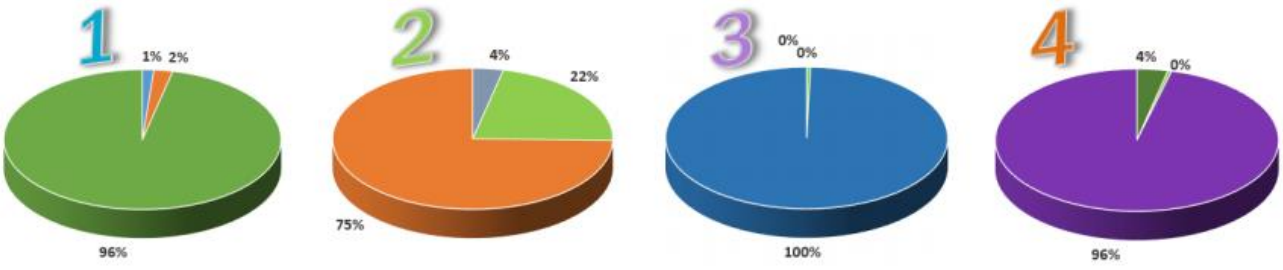
3.2 Medidas de Implementação do PIT

Implementação

AÇÕES	RECURSOS ENVOLVIDOS	PERÍODO	CONCLUSÃO
Questionário sobre Código de Ética e Conduta	DGC	até 30-abr	100%
Questionário sobre Conflito de Interesses	DGC	até 31-jul	100%
Questionário sobre o Regulamento de Utilização de Informação	DGC	até 31-out	100%
Questionário sobre o Regulamento de Utilização das Tecnologias de Informação e Comunicação	DGC	até 31-dez	100%

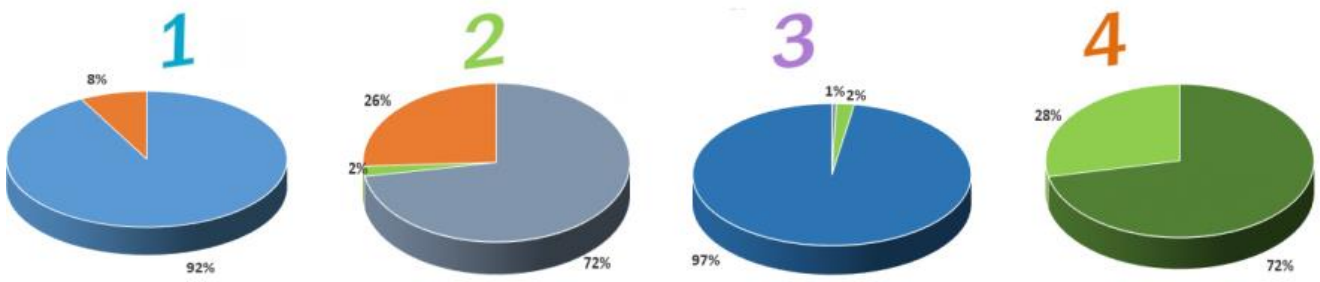
3.2.1 Resultados do questionário sobre o Código de Ética e Conduta

Do universo de trabalhadores do Instituto de Informática, I.P., 267 responderam ao questionário, tendo 228 respondido à totalidade das questões.



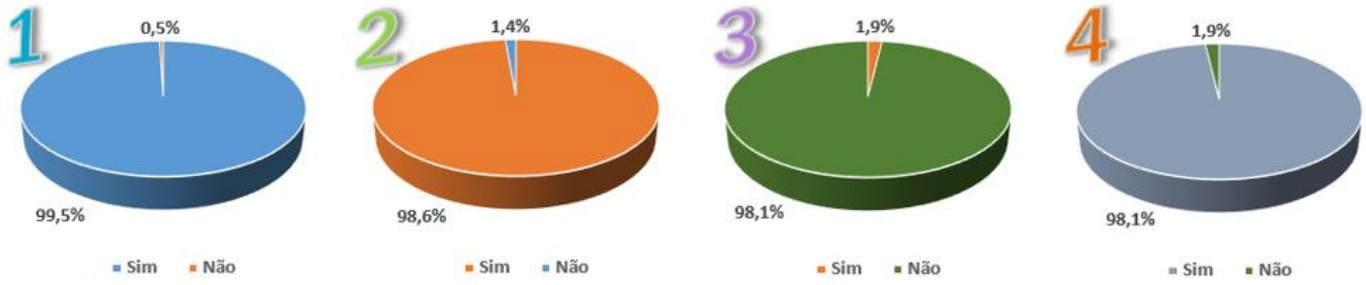
3.2.2 Resultados do questionário sobre o Plano de Prevenção de Riscos de Corrupção e Infrações Conexas – Conflito de Interesses

Do universo de trabalhadores do Instituto de Informática, I.P., 241 responderam ao questionário, tendo 194 respondido à totalidade das questões.



3.2.3 Resultados do questionário sobre o Regulamento de Utilização de Informação

Do universo de trabalhadores do Instituto de Informática, I.P., 230 responderam ao questionário, tendo 211 respondido à totalidade das questões.



3.3 Medidas de redução dos riscos de corrupção e infrações conexas

As medidas de prevenção que foram estabelecidas, em função do grau de risco, são alvo de verificações internas regulares, com vista à eliminação ou mitigação dos principais riscos.

Não obstante a existência destas ações, todos os trabalhadores do II, I.P., internos e externos, devem atuar respeitando as regras inerentes às suas funções, respeitar a confidencialidade dos dados a que têm acesso no desempenho daquelas funções e agir sempre em conformidade com a Lei e de acordo com as normas previstas no PIT.

Em seguida é apresentada a avaliação do estado de implementação das medidas estabelecidas.

Área de Organização do DOGP

Contratação da Aquisição de Bens e Serviços

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Favorecimento de fornecedores	Elevado	- Divulgação do Regulamento de Compras e CCP.	85%	31-12-2019
		- Criação de controlo interno ao nível da despesa.	100%	
		- Avaliação da relevância e oportunidade das aquisições.	100%	
Tráfico de influência	Elevado	- Avaliação periódica de fornecedores.	100%	
		- Esquema sequencial hierarquizado de aprovação e autorização no decurso da Aquisição.	100%	
Fracionamento de despesa	Elevado	- Segregação de funções.	100%	
		- Verificação automática dos fornecedores de forma a evitar a possibilidade de repetição.	100%	
Não cumprimento do regime de exceção previsto no DL n.º 278/2009, de 2/10	Elevado	- Controlo da legalidade pelos assessores jurídicos.	100%	
Realização de despesas sem cabimento prévio	Elevado	- Aumento da rotatividade de fornecedores.	100%	
Deficiente ou insuficiente definição dos critérios de adjudicação ou qualificação.	Elevado	- Definição de modelo tipo para ajuste direto.	100%	
Insuficiente fundamentação do recurso ao Ajuste Direto	Elevado			
No âmbito do ajuste direto, convidar entidades a apresentar propostas que tenham excedido os limites definidos no art.º 113 do CCP	Elevado			
Conflito de interesses por quem participou na elaboração da proposta.	Elevado	- Rotatividade dos Júris.	100%	
Admissão de propostas extemporâneas ou de entidades com impedimentos legais	Elevado	- Obrigatoriedade de consultar três fornecedores no ajuste direto.	100%	
Conflito de interesses dos elementos que integram o júri	Elevado	- Ampla divulgação do regime de impedimentos;	100%	
Não audição dos concorrentes quando há lugar a exclusão /relatório preliminar	Elevado			

Deficiente exercício do poder discricionário na avaliação das propostas/candidaturas	Elevado	- Subscrição de uma declaração de Compromisso relativa a incompatibilidades, impedimentos, escusa e suspeição, caso se verifique.	100%	
Contenham cláusulas ilegais	Elevado			
Deficiente ou insuficiente definição das cláusulas de penalização contratuais em caso de não cumprimento das obrigações por ambas as partes	Elevado			
Falta de correspondência entre as cláusulas contratuais e as definidas nas peças do respetivo concurso	Elevado			

Receção de Bens e Serviços

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Desvio ou não fiscalização da quantidade e qualidade dos bens e serviços.	Elevado	- Promoção de verificações aleatórias, por amostragem, a um número mínimo de processos.	100%	(1)
Retenção de material para uso próprio do Trabalhador.	Elevado	- Revisão das regras de controlo interno.	100%	

(1) - Verificação IAF/SIF.

Gestão Económica e Financeira

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Insuficiências ao nível da inventariação e avaliação contabilística dos bens.	Elevado	Reforço das ações de verificação e auditoria	94%	31-12-2019 (2)
Insuficiente controlo interno na área do aprovisionamento quanto à execução dos concursos, e gestão de contratos.	Elevado	Considerar padrões rigorosos de desempenho e responsabilização pelos trabalhadores	100%	

(2) – Para bens de 2013 a 2016 - fonte de verificação SIF-SAP.

Área de Gestão de Pessoas do DOGP

Recrutamento e Seleção

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Designação de elementos que integrem os júris dos procedimentos concursais, que possam por impedimento ou suspeição prevista nos artigos 69.º e seguintes do CPA, pôr em risco a isenção dos resultados.	Elevado	- Rotatividade dos funcionários designados para constituição de júris.	100%	
		- Adequação dos métodos de seleção ao perfil do cargo.	100%	
		- Definição clara das funções / perfis e competências	100%	
		- Regras específicas do recrutamento.	100%	

Gestão das Necessidades de Recursos

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Recurso a trabalho suplementar, contratações a termo ou a prestações de serviços, como forma de suprir necessidades permanentes dos serviços.	Elevado	- Identificar por área e função os recursos externos afetos.	100%	
		- Planeamento anual das necessidades do serviço, de forma a recrutar trabalhadores recorrendo a figuras legalmente consagradas tais como concursos de pessoal.	100%	

Acumulação de Funções

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Acumulação de funções públicas ou/e privadas ilegais ou sem autorização superior.	Moderado	- Registar todos os pedidos de acumulação de funções privadas/públicas numa base de dados.	100%	
		- Divulgar internamente as acumulações de funções registadas e definir uma periodicidade para revisão.	75%	31-03-2019

Tempos de Trabalho

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO
Incumprimento do horário estabelecido.	Moderado	- Envio de mapas mensais com o registo de situações irregulares ao superior hierárquico e solicitar às entidades competentes a eventual verificação domiciliária, sempre que se justifique.	100%
Existência de faltas não justificadas.	Moderado	- Definir procedimento disciplinar a adotar em caso de consecutivas situações de faltas não justificadas e/ou incumprimento de horário.	100%

Processamento de Vencimentos e Abonos

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Irregularidades/falhas no processamento de vencimentos e abonos dos trabalhadores.	Elevado	- Assegurar a segregação de funções no processamento de vencimentos e abonos dos trabalhadores garantindo a intervenção no processo de processamento e entrega de dois ou mais intervenientes.	100%	
		-Elaborar e divulgar Manual de Processamento de vencimentos e abonos.	50%	31-06-2019

Necessidades Formativas

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Desajustamento entre as necessidades de formação e a formação efetivamente fornecida.	Elevado	- Adoção de medidas de gestão previsional com vista a ajudar a identificar e prover as necessidades formativas das unidades orgânicas.	100%	
		- Executar procedimentos com a finalidade de garantir o aproveitamento das ações de formação e assegurar a difusão dos conhecimentos pelos formandos.	100%	
		- Associação da identificação das necessidades formativas aos momentos de avaliação de desempenho e à função /matriz de competências.	50%	31-12-2019
		- Criação de uma base de dados com o registo do percurso formativo por colaborador, função e habilitações académicas.	80%	31-12-2019 (3)
		- Avaliação do processo formativo.	100%	
Financiamento de ações de formação a trabalhadores em funções públicas, por entidades privadas para obter vantagens ilícitas.	Elevado	- Controlo/identificação das entidades privadas que financiam formações aos trabalhadores/formandos	100%	
Recurso a formação prestada por entidades privadas não acreditadas.	Fraco	- Controlo e registo das empresas que dão formação.	100%	
Baixa execução do Plano Anual de Formação.	Elevado	- Envolvimento das unidades orgânicas no planeamento e na definição das necessidades de formação dos Recursos Humanos;	100%	
		- Definição e divulgação do Procedimento de elaboração, implementação e monitorização do Plano de Formação Anual.	100%	
		- Acompanhamento e controlo da implementação do Plano de Formação pela AGP.	100%	

(3) – Falta atualizar as habilitações literárias de alguns trabalhadores.

Avaliação de Desempenho

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Ausência de mecanismos explícitos que identifiquem e impeçam a ocorrência de conflitos de interesses.	Elevado	- Criar normas para prevenção de conflitos de interesse	100%	
Exercício ilegal da discricionariedade no processo de avaliação dos trabalhadores.	Elevado	- Definir *à priori* os critérios de aplicação das quotas de relevante e excelente	100%	

Acidentes de Trabalho "*in itinere*"

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO
Falsas declarações.	Fraco	- Exigência de apresentação de comprovativos, e se necessário, processo de averiguações.	100%

Acidentes de Trabalho "*in itinere*"

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO
Não atualização dos dados pessoais dos trabalhadores em funções públicas.	Elevado	- Revisão periódica dos dados pessoais dos trabalhadores.	100%
Interferência ilegal nas bases de dados pessoais dos trabalhadores em funções públicas	Elevado		

Diretor de Segurança de Informação[2]

Segurança da Informação

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Manipulação de dados/fornecimento de informação a terceiros/abuso de confiança/favorecimento próprio ou de terceiros.	Elevado	- Criar e implementar o plano de segurança da organização – Política, normas, guiões e procedimentos.	100%	(4)
		- Definir e atribuir a gestão da segurança na organização.	100%	
		- Definir e atribuir a responsabilidade no acesso e tratamento dos dados e dos sistemas informáticos.	100%	(5)
		- Revisão e atualização do Sistema de Gestão de Segurança de Informação.	100%	(6)
		- Criar procedimentos para classificar a informação.	100%	(7)

(4) – AI2016-01 - Aprovação e publicação políticas segurança.
(5) – Procedimento de gestão de acessos.
(6) – AI2016-01.
(7) - Política PSISS D-2.

[2] As competências funcionais do Diretor de Segurança de Informação foram assumidas pela Área de Segurança da Informação e Proteção de Dados Pessoais por Deliberação n.º 11/CD/2018, de 30 de maio.

Aquisição de Produtos de Software

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Aquisição /Utilização inadequada de produtos de software.	Elevado	- Definir normas, regras e procedimentos de aquisição e utilização de produtos de software, considerando, nomeadamente, o cumprimento legal de requisitos de licenciamento e direitos de copyright, bem como os princípios de racionalização de custos e recurso a produtos open source.	100%	(8)

(8) – PCD031 - Procedimentos de utilização aceitável de software e hardware.

Área da Qualidade e Auditoria

Auditoria e Controlo Interno

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Omissão de ações de controlo em áreas ou serviços determinados.	Elevado	- Identificação/declaração de conflito de interesses de auditores e dirigentes	100%	(9)
		- Critérios objetivos de seleção das ações a realizar.	100%	
		- Duplo grau de apreciação/decisão dos relatórios das ações de controlo.	100%	
Favorecimento ou ocultação de situações irregulares no âmbito das auditorias e ações desenvolvidas junto das unidades auditadas.	Elevado	- Avaliação da Qualidade das Ações.	100%	
Prática de atos com violação dos deveres funcionais relacionados com situações de conflito de interesses.	Elevado	- Aprovação e divulgação de Normas de Boas Práticas, com vista à adoção de uma cultura de legalidade, clareza e transparência nos procedimentos de auditoria.	100%	(10)

(9) – Manual de segregação de Funções.

(10) – Procedimento Auditorias Internas (versão 7.0) que foi revisto a 08.10.2018. Procedimento de acordo com o descrito na norma portuguesa ISO 19011 – Linhas de Orientação para Auditorias a Sistemas de Gestão.

Gabinete Jurídico

GJ - Contratação da aquisição de Bens e Serviços

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO	
Elaboração de peças procedimentais com requisitos passíveis de privilegiar ou excluir determinadas entidades.	Elevado	- Definição de modelos tipo de contrato por tipo serviço/bens a adquirir	100%	

3.4 Medidas de Prevenção ao Conluio na Contratação Pública

DOGP/AO - Contratação da Aquisição de Bens e Serviços

RISCO IDENTIFICADO	RISCO	MEDIDAS	CONCLUSÃO
Conluio na contratação pública	Elevado	- Implementar procedimentos de deteção (reativa e proativa) e de prevenção.	100%
		- Sensibilizar os trabalhadores e promover o escrutínio da informação.	100%
		- Reduzir a previsibilidade dos procedimentos.	100%

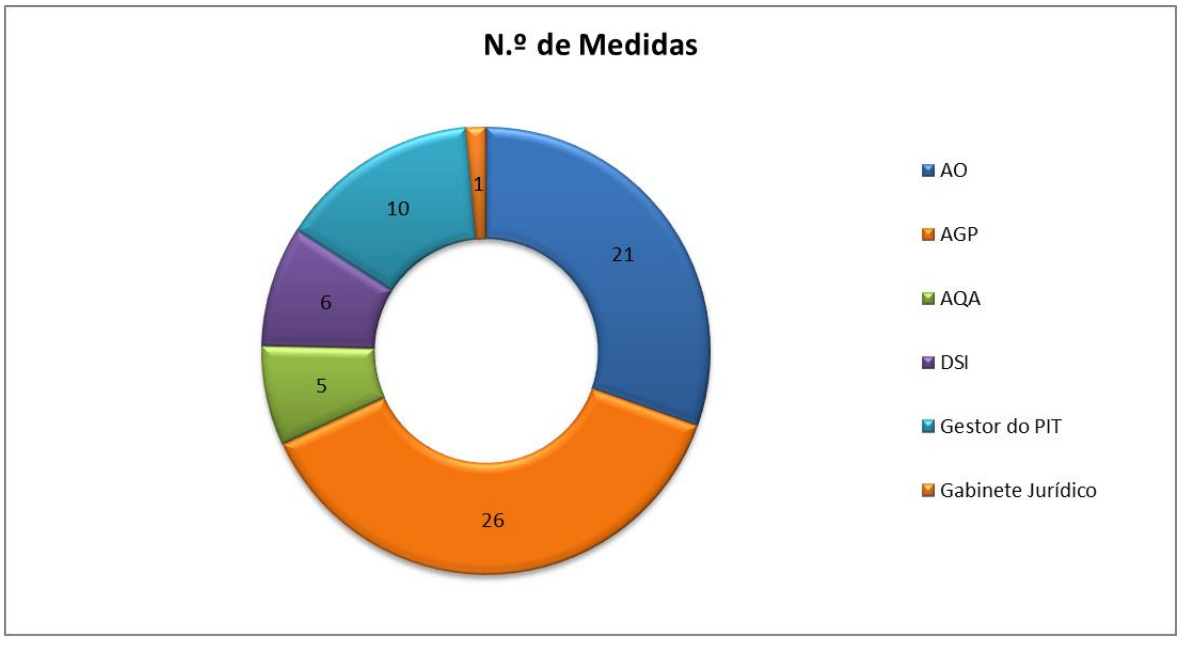
4. Conclusões

Na sua essência, os quadros apresentados evidenciam uma sistematização da implementação das medidas do Plano de Integridade e Transparência.

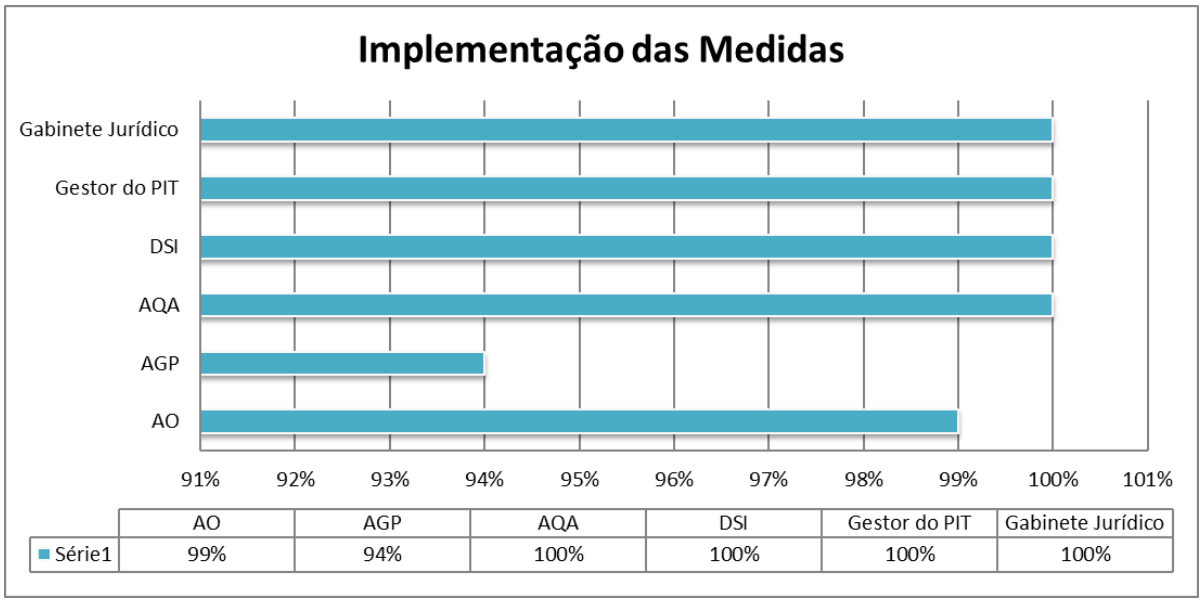
Foram realizadas ações de formação, reflexão e sensibilização, junto dos trabalhadores, tendo por objeto a sistematização dos instrumentos do Plano de Integridade e Transparência, designadamente do Plano de Prevenção de Riscos de Corrupção e Infrações Conexas, do Código de Ética e de Conduta, do Regulamento de Utilização de Informação, do Regulamento de Utilização das TIC e do Código de Conduta de Fornecedores, com especial enfoque na divulgação de boas-práticas na prossecução do serviço público e na sensibilização dos conflitos de interesses.

Verifica-se o efeito positivo que a implementação do PIT como um todo tem tido, ao nível do desenvolvimento das atividades por parte de cada unidade orgânica, permitindo evidenciar com maior eficácia a aplicação das medidas de prevenção definidas no PIT.

Em suma, e conforme se passa a demonstrar, cerca de 99%[3] das medidas propostas, encontram-se implementadas.



[3] À data de dezembro de 2018.


Implementação das Medidas
Gabinete Jurídico
Gestor do PIT
DSI
AQA
AGP
AO
91%
92%
93%
94%
95%
96%
97%
98%
99%
100%
101%
AO
AGP
AQA
DSI
Gestor do PIT
Gabinete Jurídico
Série1
99%
94%
100%
100%
100%
100%

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