Aprovado pelo
Conselho Diretivo
em 28 de Outubro de 2025

Divulgue-se

Dra. Maria Antónia Escoval
Presidente do Conselho Diretivo

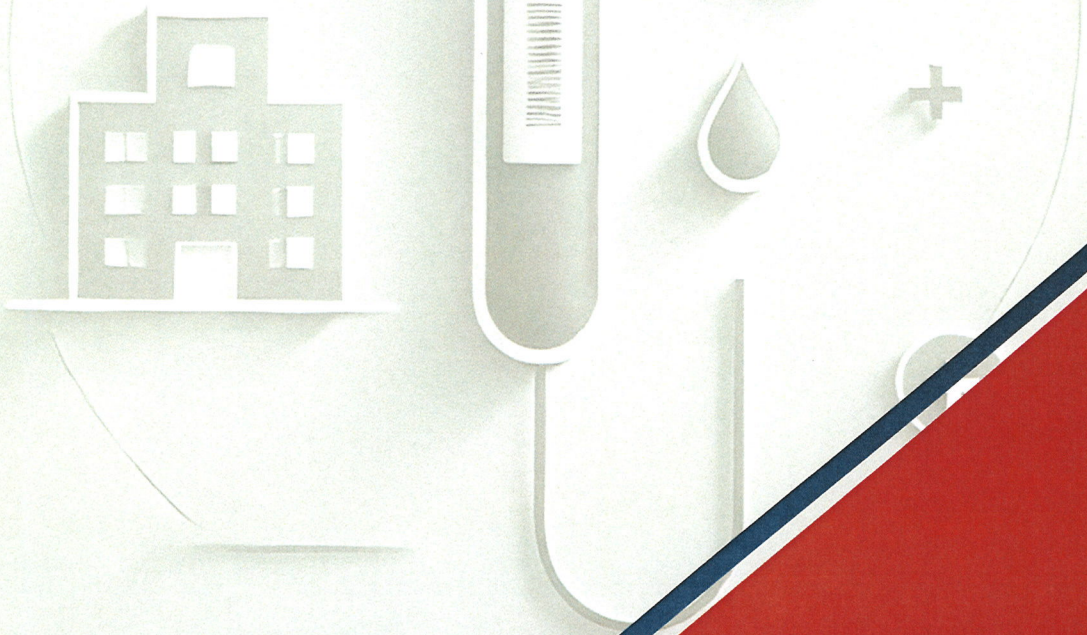
Dr. Victor Marques
Vogal do Conselho Diretivo

RELATÓRIO INTERCALAR

Avaliação e Execução do Plano de Prevenção de Riscos de Corrupção e Infrações Conexas

Instituto Português do Sangue e da Transplantação

Outubro | 2025



www.ipst.pt

Revisão Nº. | Data

REPÚBLICA PORTUGUESA
SAÚDE

SNS
SERVIÇO NACIONAL DE SAÚDE

IP ST
Instituto Português do Sangue e da Transplantação, IP

Moradas

Instituto Português do Sangue e da Transplantação

IPST,IP | Serviços Centrais
Avenida Miguel Bombarda, 6 | 1000-208 Lisboa

Lisboa | Área Funcional do Sangue
Parque de Saúde de Lisboa, Av. do Brasil, n.º 53 – Pav. 17 | 1749-005 Lisboa

Lisboa | Área da Transplantação
Alameda das Linhas de Torres, nº 117 |1769-001 Lisboa

Algarve| Área Funcional do Sangue | LRSP Dra. Laura Ayres
Parque das Cidades, S. João da Venda, Loulé / Faro | 8135-014 Almancil

Coimbra | Área Funcional do Sangue | Área da Transplantação
Rua Escola Inês de Castro, São Martinho do Bispo | 3040-226 Coimbra

Porto | Área Funcional do Sangue | Área da Transplantação
Rua do Bolama, nº 133 | 4200-139 Porto

A Comissão de Prevenção da Corrupção | Coordenação

Délia Falcão
Tlf: +351 220 045 204
@: Delia.Falcao@ipst.min-saude.pt

A Comissão de Prevenção da Corrupção | Equipa

Alberto Matias
Tlf: +351 210 063 275
@: Alberto.Matia@ipst.min-saude.pt

Clara Vitoriano
Tlf: +351 210 063 225
@: Clara.Vitoriano@ipst.min-saude.pt

Graça Fonseca
Tlf: +351 220 045 205
@: Graca.Fonseca@ipst.min-saude.pt

Raquel Gomes
Tlf: +351 210 064 232
@: Raquel.Gomes@ipst.min-saude.pt

Ana Mendes
Tlf: +351 220 045 204
@: Ana.Mendes@ipst.min-saude.pt

Francisco Ferreira Pinto
Tlf: +351 217 921 045
@: Francisco.Pinto@ipst.min-saude.pt

Paulo Moura
Tlf: +351 220 045 230
@: Paulo.Moura@ipst.min-saude.pt

Lisboa | 24 de outubro de 2025

Índice

Índice de Figuras

Índice de Gráficos

INTRODUÇÃO

O presente relatório dá cumprimento ao Decreto-Lei n.º 109-E/2021, de 9 de dezembro, que determina na alínea a) do n.º 4 do artigo 6.º, a elaboração no mês de outubro de um relatório de avaliação intercalar nas situações identificadas de risco elevado ou muito elevado (máximo) no Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PPR).

A avaliação intercalar constitui uma ferramenta fundamental para monitorizar a implementação das medidas definidas no plano, identificar áreas críticas e promover o aperfeiçoamento contínuo do sistema de gestão de riscos.

Este documento estrutura-se de forma a apresentar o estado atual de execução, analisar os resultados obtidos e propor ajustamentos que consolidem a eficácia das ações implementadas.

No ano de 2025 foi implementado o PPR 2025 do IPST, já revisto de acordo com o Regulamento Geral da Prevenção da Corrupção (RGPC) e as orientações do Mecanismo Nacional Anti-Corrupção (MENAC), bem como as alterações decorrentes da evolução da orgânica ou outras consideradas relevantes.

ENQUADRAMENTO

O IPST, IP é um Instituto Público integrado na administração indireta do Estado, dotado de autonomia técnica, administrativa e financeira, com património próprio (cf. artigo 1.º, n.º 1, do Decreto-Lei n.º 39/2012, de 16 de fevereiro). Sob a superintendência e tutela do Ministro da Saúde, o IPST tem jurisdição em todo o território nacional, com sede em Lisboa.

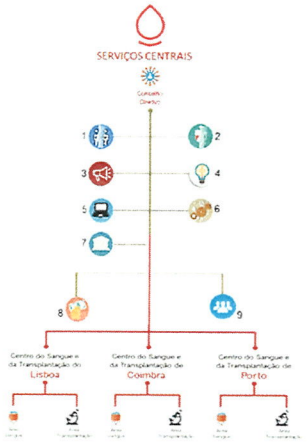
Enquanto organismo central do Serviço Nacional de Saúde (SNS), nos termos do n.º 1, alínea e), do artigo 3.º do Decreto-Lei n.º 52/2022, de 4 de agosto, o IPST tem como missão garantir a segurança, qualidade e eficiência na gestão de componentes biológicos, incluindo sangue, tecidos, células e órgãos. A sua atuação abrange atividades como colheita, processamento, armazenamento, distribuição e análise de componentes biológicos, desempenhando um papel central na prestação de cuidados de saúde.

O IPST é também responsável por promover a formação, a investigação científica e a inovação no setor da saúde, contribuindo para o aperfeiçoamento contínuo do sistema nacional de saúde.

A sua orgânica e estrutura estão definidas no Decreto-Lei n.º 39/2012, de 16 de fevereiro, e na Portaria n.º 165/2012, de 22 de maio.

O IPST trabalha em conformidade com normas nacionais e europeias, permitindo desempenhar um papel de referência na saúde pública, em alinhamento com os princípios de transparência, legalidade e responsabilidade institucional.

***Figura 1** - Organograma Institucional*



- Coordenação Nacional da Transplantação **(CNT)**
- Coordenação Nacional do Sangue e da Medicina Transfusional **(CNSMT)**
- Gabinete de Comunicação, Promoção da Dádiva e Voluntariado **(GCPDV)**
- Gabinete de Investigação, Inovação e Desenvolvimento **(GIID)**
- Gabinete de Tecnologias de Informação e Comunicações **(GTIC)**
- Gabinete de Gestão da Qualidade **(GGQ)**
- Gabinete Jurídico **(GJ)**
- Departamento de Planeamento e Gestão Patrimonial e Financeira **(DPGPF)**
- Departamento de Gestão de Recurso Humanos e Formação **(DGRHF)**
- Centros de Sangue e da Transplantação **(CST's)**

AVALIAÇÃO INTERCALAR

METODOLOGIA

O Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PPR) tem como referência para a definição do risco, como o evento, situação ou circunstância futura com probabilidade de ocorrência e potencial consequência positiva ou negativa na obtenção dos objetivos de uma entidade ou organização.

Para a análise destes riscos, existem escalas próprias de Possibilidade de Ocorrência e Impacto, alinhadas com os objetivos de gestão dos Riscos de Corrupção e Infrações Conexas.

ÂMBITO

A avaliação intercalar foca-se em situações identificadas de risco elevado ou máximo, quantificando o grau de implementação das medidas preventivas e corretivas já adotadas, além de prever a sua completa implementação em conformidade com o nº4 do artigo 6º do Regime Geral da Prevenção da Corrupção, conforme estabelecido pelo Decreto-lei nº 109-E/2021, de 9 de dezembro.

A identificação e a graduação dos riscos foram realizadas com a colaboração dos Diretores, Gestores e responsáveis, que reportaram o nível de execução de cada uma das medidas de mitigação em vigor no ano de 2025. As matrizes de risco foram minuciosamente analisadas, incluindo as áreas designadas no organograma institucional (***Figura 1***).

Aquando do relatório anual de 2025 do PPR do IPST, IP em vigor, procedeu-se a uma revisão do grau de riscos, em concreto referente ao DPGPF e DGRHF e GTIC, alguns dos riscos desceram do

grau elevado para moderado, em virtude da adoção de novas medidas de mitigação e de correção e em particular quanto a este último da criação da Comissão de Cibersegurança do IPST, IP.

No entanto, no presente relatório foi necessário rever os riscos e medidas tanto no DPGPF e no DGRHF devido a ocorrências verificadas, conforme representado graficamente.

O PPR do IPST em vigor identificou 8 riscos elevados inerentes às atividades desenvolvidas pelas unidades orgânicas (UO), e 18 medidas para mitigação desses mesmos riscos, cuja situação se encontra sintetizada no Quadro 1.

Quadro 1 - Síntese Avaliação Intercalar de Risco Elevado e Muito Elevado (máximo) e respetivas medidas preventivas PPR, 2025

UO	Riscos Elevados	Medidas	Implementadas	Em Implementação
Transversais a todas UO	2	3	2	2
GTIC	4	14	11	2
CST's	2	2	0	2
TOTAL	8	18	13	6

Em outubro de 2025, das 18 medidas previstas no PPR para mitigação de Risco Elevado, encontravam-se 13 implementadas. Conforme apresentado no quadro seguinte:

Quadro 2 - Avaliação Intercalar PPR 2024 | Síntese dos Riscos identificados de Grau Elevado

Unidade Orgânica	ATIVIDADE	AREA DE RISCO	GRADUAÇÃO DE RISCO			MEDIDAS DE PREVENÇÃO	Implementação		
			PO	IP	GR		Sim	Não	Em Curso
Transversal	Proteção de Dados Pessoais	Divulgação indevida, interna ou externa, em proveito próprio ou de terceiro, de dados pessoais acessíveis no exercício de funções.	2	3	Elevado	Ministrar ações de formação.			X
						Monitorizar e identificar situações desconformes.	X		
		Celebração de contratos / protocolos sem garantir o respeito pela Política de Privacidade do IPST e a proteção dos dados pessoais	2	3	Elevado	Compilar e rever os contratos com fornecedores e protocolos em vigor.			X
GTIC	Requisitos de segurança das redes e sistemas de informação e notificação de incidentes.	Articulação insuficiente com o Centro Nacional de Cibersegurança (CNCS)	2	3	Elevado	Indicar o ponto de contacto permanente com o CNCS para assegurar os fluxos de informação de nível operacional e técnico.	X		
						Designar o responsável de segurança para a gestão das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes, nos termos do Regime Jurídico da Segurança do Ciberespaço e do Decreto Lei n.º 65/2021, de 30 de julho.	X		
						Identificar e descrever as medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes.	X		
						Elaborar o relatório anual de segurança, a remeter ao CNCS.	X		
	Controlo da segurança: Disponibilidade, integridade e confidencialidade da informação residente nos sistemas de informação/ Utilização e exploração do ciberespaço.	Falha de segurança nos sistemas de informação do IPST	2	3	Elevado	Realizar uma análise de risco dos ativos tecnológicos físicos e de informação, essenciais ao funcionamento do IPST.	X		
						Rever e atualizar a Política de Segurança da Informação do IPST (definição e implementação de restrições físicas, controlo de acessos a equipamentos e instalações, autorização e rastreabilidade na autenticação aos sistemas).	X		
						Condicionar o acesso físico ao Data Center, assegurando um acesso restrito e controlado.			X
		Risco de erros na operação de sistemas e manuseamento da informação, falhas e interrupções na disponibilização da informação e comunicações.	2	3	Elevado	Rever e atualizar a Política de Segurança da Informação no IPST (definição e implementação de medidas de proteção física e lógica dos equipamentos e da informação).	X		
						Atualizar os procedimentos de salvaguarda (backup) e recuperação (restore) de informação e os de segurança no acesso ao armazenamento de dados.	X		
						Elaborar plano/s de contingência.	X		
		Falhas na segurança decorrente da livre circulação de dispositivos (local de trabalho, serviço externo, domicílio).	2	3	Elevado	Assegurar o inventário de todos os equipamentos de tecnologias de informação, o respetivo registo no sistema de inventário e a atualidade do registo de afetação aos Dirigentes e trabalhadores/as.	X		
						Assegurar a proteção da informação residente nos computadores (desktops e laptops) através de mecanismos de cifra dos discos, controlo de acessos de sessão (login), controlo de acessos por rede ao computador (firewall), atualização do sistema operativo e antivírus e estabelecimento de ligações seguras à rede do IPST (VPN).	X		
						Implementar mecanismos de controlo de ligação à rede do IPST de equipamentos estranhos não autorizados.	X		
						Realizar ações de formação e sensibilização sobre cibersegurança e segurança da informação.			X
CST's	NPGPF	Entrada e saída de bens não autorizada e abates sem autorização	2	3	Elevado	Cumprimento do Manual de Procedimentos do Departamento de Planeamento e Gestão Patrimonial e Financeira.			X
		Apropriação ou uso ilegítimo, de bens, fundos ou valores confiados aos trabalhadores no exercício das suas funções	2	3	Elevado	Cumprimento do Manual de Procedimentos do Departamento de Planeamento e Gestão Patrimonial e Financeira.			X

Sem prejuízo das medidas, supra, cabe destacar as seguintes medidas **em implementação** para mitigação de Riscos Elevados transversais a toda a instituição:

Gestão e perfis de acessos dos utilizadores

O IPST tem continuado a prosseguir uma política de reforço da segurança dos sistemas informáticos. A gestão e perfis de acesso dos utilizadores encontra-se definida de acordo com os diferentes perfis de utilizador (administradores, utilizadores regulares, convidados, entre outros) com permissões específicas. Este aspeto tem vindo a ser aperfeiçoado. Existe igualmente a implementação de regras de modo a garantir a criação de perfis e permissões, assim como o seu cancelamento.

Pretende-se futuramente que os acessos sejam auditados regularmente de forma a identificar acessos indevidos ou desnecessários, bem como a revisão e remoção dos acessos de utilizadores inativos ou que já não pertencem à organização, assegurando assim uma monitorização e uma qualidade permanente.

Pretende-se em simultâneo dar continuidade às medidas de controlo de gestão e perfis de acesso através da implementação de medidas como: controlo de acesso baseado em funções, para garantir que os utilizadores só acedem às informações necessárias para as suas funções e autenticação de dois fatores para aumentar a segurança.

Aplicação de regras de confidencialidade

O IPST, dispõe de uma Política de Proteção de Dados e Privacidade e cumpre com as normas jurídicas comunitárias e nacionais aplicáveis no âmbito da proteção de dados, da privacidade e da segurança da informação. Estas matérias são cada vez mais de natureza sensível, estando o IPST atento e empenhado no sentido de melhorar as suas práticas, designadamente:

- Melhorar os procedimentos relativos às regras e boas práticas de proteção de informações sensíveis;
- Ministrar formação aos colaboradores: Realizar formações periódicas sobre a importância da confidencialidade e como a garantir em função de cada área e sector e departamento;
- Estatuir a assinatura de acordos de confidencialidade: Requerer aos colaboradores, fornecedores e parceiros a assinatura de NDA (Non-Disclosure Agreements).

Medidas de segurança de informação

O IPST dispõe de planos de recuperação e backup, encontram-se estabelecidos backups regulares e um plano de recuperação para minimizar impactos em caso de incidentes. É ainda realizada uma monitorização contínua, utilizando as ferramentas disponíveis para detetar atividades anómalas na rede e sistemas.

Acesso controlado à informação e documentação

O IPST prossegue o processo continuo de implementação de medidas de segurança para o acesso controlado à informação e documentação. Ao nível digital, encontram-se implementados nalguns dos softwares utilizados (Ex. ASIS; SIRIUS; …), os sistemas de gestão documental (DMS), sendo possível utilizar software para rastrear o utilizador que acedeu, modificou ou partilhou documentos. Nos restantes softwares (Glintt; RHV; …) está em curso a implementação de rastreabilidade dos utilizadores.

Declaração de Inexistência de Conflito de Interesses

Em 2025, o IPST procedeu à revisão do Código de Conduta de Prevenção da Corrupção, que determina a assinatura de "Declaração de Inexistência de Conflito de Interesses" por todos os trabalhadores e trabalhadoras, e visa reforçar o conhecimento e o comprometimento de todos para com os valores e princípios do IPST, bem como atuar como forma de mitigação de situações de conflito de interesses.

Pedidos de acumulação de funções privadas e públicas

De realçar que a Comissão de Controlo interno procedeu no decurso de 2025, à análise de todas as situações de acumulação de funções privadas e públicas.

Importa no presente relatório, levar em consideração as contingências seguintes:

Por um lado, tendo em conta que não se verificaram ocorrências relativamente aos riscos classificados como Grau de Risco Elevado ou Muito Elevado (máximo) nomeadamente na área do GTIC, procedeu-se à redução do nível de Probabilidade de Ocorrência (PO) do risco, e, consequentemente o Grau do Risco na respetiva Matriz.

Ações a tomar:

Por outro, tendo sido detetados riscos nos DGRHF e DPGPF, procede-se neste, à alteração do nível de probabilidade de Ocorrência e, consequentemente o Grau do Risco na respetiva Matriz.

Por essas razões procede-se à apresentação de nova matriz de risco no quadro seguinte.

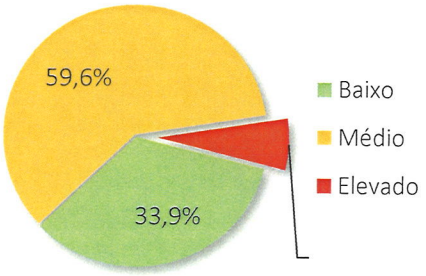
Quadro 3 - Matriz de Risco atualizada

Unidade Orgânica	ATIVIDADE	AREA DE RISCO	GRADUAÇÃO DE RISCO			MEDIDAS DE PREVENÇÃO	Implementação		
			PO	IP	GR		Sim	Não	Em Curso
Transversal	Proteção de Dados Pessoais	Divulgação indevida, interna ou externa, em proveito próprio ou de terceiro, de dados pessoais acessíveis no exercício de funções.	2	3	Elevado	Ministrar ações de formação.			X
						Monitorizar e identificar situações desconformes.	X		
		Celebração de contratos / protocolos sem garantir o respeito pela Política de Privacidade do IPST e a proteção dos dados pessoais	2	3	Elevado	Compilar e rever os contratos com fornecedores e protocolos em vigor.			X
GTIC	Requisitos de segurança das redes e sistemas de informação e notificação de incidentes.	Articulação insuficiente com o Centro Nacional de Cibersegurança (CNCS)	1	3	Moderado	Indicar o ponto de contacto permanente com o CNCS para assegurar os fluxos de informação de nível operacional e técnico.	X		
						Designar o responsável de segurança para a gestão das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes, nos termos do Regime Jurídico da Segurança do Ciberespaço e do Decreto Lei n.º 65/2021, de 30 de julho.	X		
						Identificar e descrever as medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes.	X		
						Elaborar o relatório anual de segurança, a remeter ao CNCS.	X		
GTIC	Controlo da segurança: Disponibilidade, integridade e confidencialidade da informação residente nos sistemas de informação/ Utilização e exploração do ciberespaço.	Falha de segurança nos sistemas de informação do IPST	1	3	Moderado	Realizar uma análise de risco dos ativos tecnológicos físicos e de informação, essenciais ao funcionamento do IPST.	X		
						Rever e atualizar a Política de Segurança da Informação do IPST (definição e implementação de restrições físicas, controlo de acessos a equipamentos e instalações, autorização e rastreabilidade na autenticação aos sistemas).	X		
						Condicionar o acesso físico ao Data Center, assegurando um acesso restrito e controlado.			X
		Risco de erros na operação de sistemas e manuseamento da informação, falhas e interrupções na disponibilização da informação e comunicações.	1	3	Moderado	Rever e atualizar a Política de Segurança da Informação no IPST (definição e implementação de medidas de proteção física e lógica dos equipamentos e da informação).	X		
						Atualizar os procedimentos de salvaguarda (backup) e recuperação (restore) de informação e os de segurança no acesso ao armazenamento de dados.	X		
						Elaborar plano/s de contingência.	X		
		Falhas na segurança decorrente da livre circulação de dispositivos (local de trabalho, serviço externo, domicílio).	1	3	Moderado	Assegurar o inventário de todos os equipamentos de tecnologias de informação, o respetivo registo no sistema de inventário e a atualidade do registo de afetação aos Dirigentes e trabalhadores/as.	X		
						Assegurar a proteção da informação residente nos computadores (desktops e laptops) através de mecanismos de cifra dos discos, controlo de acessos de sessão (login), controlo de acessos por rede ao computador (firewall), atualização do sistema operativo e antivírus e estabelecimento de ligações seguras à rede do IPST (VPN).	X		
						Implementar mecanismos de controlo de ligação à rede do IPST de equipamentos estranhos não autorizados.	X		
						Realizar ações de formação e sensibilização sobre cibersegurança e segurança da informação.			X
CST's	NPGPF	Entrada e saída de bens não autorizada e abates sem autorização	2	3	Elevado	Cumprimento do Manual de Procedimentos do Departamento de Planeamento e Gestão Patrimonial e Financeira.			X
		Apropriação ou uso ilegítimo, de bens, fundos ou valores confiados aos trabalhadores no exercício das suas funções	2	3	Elevado	Cumprimento do Manual de Procedimentos do Departamento de Planeamento e Gestão Patrimonial e Financeira.			X
DGRHF	Recrutamento e Seleção de Pessoal	Quebra de deveres de transparência e imparcialidade.	3	2	Elevado	Rotatividade dos elementos designados para constituição de Júris			X
						Adequação dos métodos de seleção ao perfil do cargo privilegiando sempre que possível a prova de conhecimentos.			X
DGPGPF	Gestão dos Equipamentos	Falhas na inventariação, no abate dos bens móveis e no controlo de materiais e equipamentos, que propiciem o furto ou outras condutas ilícitas em benefício próprio ou de terceiros	2	3	Elevado	Manter atualizado o Manual de Procedimentos do Departamento de Planeamento e Gestão Patrimonial e Financeira.			X
						Realizar inventário, por amostragem, com verificações físicas trimestrais.			X

RESULTADOS

A análise da distribuição dos riscos identificados nas Unidades Orgânicas demonstra uma clara predominância de riscos classificados como baixos e moderados, representando, respetivamente, 33,9% e 59,% do total. Por outro lado, os riscos elevados correspondem a 6,4% do universo analisado, o que indica que a maioria das situações de risco não apresenta, à partida, um grau de severidade crítico (***Gráfico 1***).

Gráfico 1 *- Distribuição dos Riscos*



Face à atualização da Matriz de Riscos, no presente os riscos elevados encontram-se concentrados nas áreas transversais (2 riscos) e nas unidades dos DGRHF (1 risco) e DGRHF (1 risco), no total com 4 riscos elevados, e nos CST, que registam 2 riscos elevados, correspondendo conjuntamente a 6 riscos dos 109 riscos avaliados. Este facto sublinha a necessidade de priorizar ações corretivas e preventivas nestas áreas e departamentos, de forma a mitigar potenciais consequências mais graves.

Nas áreas transversais os riscos elevados que estão identificados são associados a áreas críticas, nomeadamente a política de gestão de dados pessoais, quanto ao DGRHF os riscos elevados surgem na atividade de recrutamento e seleção de pessoal nomeadamente na abertura de procedimento concursais, e de definição de requisitos e na composição dos júris e por outro no DPGPF estão associados à inventariação de stocks e a utilização de produtos.

Os riscos elevados reforçam a necessidade de implementar medidas de controlo mais rigorosas, garantindo a prevenção de potenciais irregularidades.

Medidas e Ações Recomendadas | Implementadas

Os riscos elevados identificados nas áreas transversais, nos DGRHF e DPGPF e nos núcleos de Gestão Patrimonial e Financeira dos CSTs foram objeto de uma abordagem estruturada, com a implementação de medidas específicas e integradas destinadas à mitigação de potenciais impactos e ao reforço do controlo e da conformidade dos processos.

Para mitigar os riscos identificados nas áreas transversais, foram definidas e implementadas as seguintes ações:

Riscos 1 e 2 **Áreas transversais a todas as Unidades Orgânicas – Proteção de dados pessoais RGPD**

1. **Divulgação indevida, interna ou externa, em proveito próprio ou de terceiro, de dados pessoais acessíveis no exercício de funções.**

- Realização de ações de formação como forma de garantir os conhecimentos em sede de RGPD e em concreto de dados pessoais sensíveis, agendadas para novembro deste ano, que terão como destinatários as chefias intermédias e outros profissionais com responsabilidade relevante nesta área;
- Realização de auditorias internas.

2. **Celebração de contratos / protocolos sem garantir o respeito pela Política de Privacidade do IPST e a proteção dos dados pessoais**

- Compilar e rever os contratos com fornecedores e protocolos em vigor.

Risco 3 **DGRHF – Recrutamento e seleção de pessoal**

- Definição de critérios e requisitos específicos exigidos nos avisos de abertura de procedimentos concursais.
- Adoção de medidas para garantir a rotatividade de elementos que compõem os Júris de concursos.
- Procedimentos na nomeação do júri dos concursos, que integre um profissional de um serviço do Instituto, diferente daquele do recrutamento, que tenha formação na metodologia das entrevistas de avaliação de competências.
- Auditorias internas
- Divulgar o código de conduta de prevenção da corrupção do IPST
- Adoção de um procedimento informático, onde fiquem registados todos os acessos dos profissionais dos RH aos processos individuais.
- Limitação de acessos aos processos individuais por utilizador às atividades de cada profissional.

Riscos 4 e 5 **DPGPF – Inventariação de bens e gestão de stocks**

3. **Entrada e saída de bens não autorizada e abates sem autorização**

- Monitorização da inventariação de bens, através da realização de auditorias internas – a realizar até 31 de dezembro de 2025.

4. **Apropriação ou uso ilegítimo de bens, fundos ou valores confiados aos trabalhadores no exercício das suas funções**

- Criação de logins pessoais nos laboratórios (nos que dispõem de sistema de login laboratorial), de forma a permitir a rastreabilidade das ações realizadas por cada colaborador até 31 de outubro de 2025;
- Formação, efetuada pelo DPGPF, dirigida aos laboratórios, para garantir o registo dos consumos de bens no momento da sua utilização no dia 10 de novembro CSTC, 14 de novembro CSTL e 17 de novembro no CSTP;
- Realização de auditorias internas, por parte do DPGPF, aos stocks existentes nos laboratórios, sem aviso prévio a decorrer até 31 de dezembro de 2025;
- Criação de um layout (com o apoio da Informática e do GGQ) relativo à produção e ao consumo de bens por atividade, permitindo monitorizar as compras e os consumos até 31 de março de 2026 em articulação com o GTIC e o GGQ.

Risco 6 **Núcleos de aprovisionamento CSTs - Inventariação de bens e gestão de stocks**

- Cumprimento do Manual de Procedimentos do Departamento de Planeamento e Gestão Patrimonial e Financeira.

Medidas Implementadas

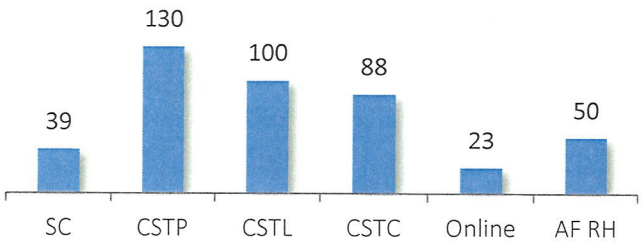
Perante os riscos elevados identificados, registou-se a implementação das medidas corretivas e preventivas. Das ações recomendadas, algumas já estão implementadas e outras encontram-se em fase de execução, conforme calendarização supra nas medidas de mitigação para cada um dos riscos, visando a redução efetiva dos riscos e o reforço dos mecanismos de controlo e conformidade. Este processo garantirá a aplicação de boas práticas, a mitigação de falhas identificadas e a promoção de uma gestão mais robusta e segura nas respetivas áreas.

Formação de Sensibilização | Esclarecimento

No ano de 2025, adicionalmente, foram realizadas ações de sensibilização sob o tema "***Breve Abordagem ao Regime Legal de Prevenção da Corrupção e Proteção dos Denunciantes de Infrações***", concebidas com o propósito de promover a consciencialização e a capacitação dos profissionais do IPST. Estas formações tiveram como objetivo principal reforçar o conhecimento sobre o enquadramento legal e as práticas associadas à prevenção da corrupção e à proteção dos denunciantes, contribuindo para o fortalecimento de uma cultura organizacional pautada pela integridade e transparência.

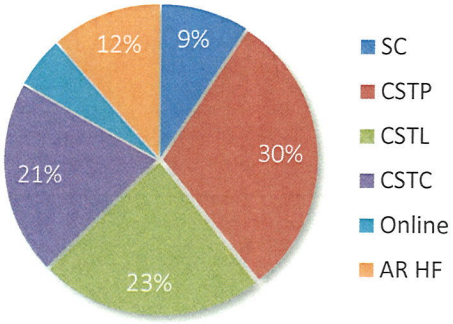
Em concreto nos dias 13, 14 e 15 de janeiro de 2025, foi promovida uma formação interna em formato misto, presencial e *online*, que contou com a participação de **380 profissionais**, conforme detalhado nos gráficos 3 e 4. Considerando que o IPST é composto por um total de 475 profissionais, estas formações acrescem às que tinham sido ministradas no ano de 2024, o que tudo perfaz os **430 colaboradores**.

Gráfico 2 - Número de Participantes da Formação



- SC (Serviços Centrais): 39 participantes
- CSTP (Centro de Sangue e da Transplantação do Porto): 130 participantes
- CSTL (Centro de Sangue e da Transplantação de Lisboa): 100 participantes
- CSTC (Centro de Sangue e da Transplantação de Coimbra): 88 participantes
- Online (Outros participantes ligados remotamente): 23 participantes
- AF RH+: 50 participantes

Gráfico 3 - Percentagem de Participantes por Unidade Orgânica



Esta iniciativa reflete o compromisso institucional do IPST em assegurar que os profissionais envolvidos possuam as competências e o entendimento necessários para atuar de forma ética e alinhada com as disposições legais, garantindo o cumprimento das melhores práticas no exercício das suas funções.

Estão previstas até final de 2025, ações de formação no âmbito do RGPD destinados quer a chefias intermédias e outros profissionais com responsabilidade relevante nesta área.

IMPLEMENTAÇÃO DA RECOMENDAÇÃO N.º 7/2024, PUBLICADA NO DR, 2ª SÉRIE, 28 DE MAIO

Dando cumprimento à referida recomendação, foram remetidos ao MENAC os reportes mensais, sendo neles identificadas as ocorrências e/ou desvios no cumprimento normativo.

CANAL DE DENUNCIA / PROCESSOS INSTAURADOS / PARTICIPAÇÕES

O canal de denuncias, procedeu quer ao registo das ocorrências recebidas, bem como do seu tratamento atempadamente.

Foi efetuada 1 denuncia anónima, por correio simples, que determinou a instauração da competente participação ao DCIAP (a decorrer) e a abertura de processo de inquérito (suspenso);

Por último, foi efetuada uma participação de ocorrência por desvio de material que originou a abertura de processo de inquérito (concluído) e subsequente participação ao DCIAP (em curso);

CONCLUSÕES

Da análise efetuada, verificou-se que no presente, das 16 medidas de prevenção previstas para as situações identificadas de risco elevado, atualmente estão em vias de implementação, maioritariamente até 31 de dezembro de 2025.

Verificou-se, no GTIC, que alguns dos riscos inicialmente de grau elevado, face por um lado à ausência de ocorrências relacionadas com os riscos identificados, e por outro lado a Criação da Comissão de Cibersegurança e subsequente atividade que, se procedeu à redução do nível de Probabilidade de Ocorrência (PO) do risco, de elevado para Moderado e, consequentemente o Grau do Risco na respetiva Matriz, passou de Grau Elevado para Moderado (quadro 3).

Acresce que estão previstas para o arranque de 2026, a reformulação da infraestrutura informática e implementação de novos processos que conduzirá a uma revisão da classificação da informação.

Já no DGRHF e DPGPF face à verificação das ocorrências supra identificadas no decurso de 2024/25, procedeu-se à correção do aumento do nível de Probabilidade de Ocorrência (PO) do risco, de 2 para 3 e, consequentemente o Grau do Risco na respetiva Matriz, passa de Moderado para Elevado (quadro 3).

Porto, 24 de outubro de 2025

Elaborado por:

Délia Falcão
Ana Mendes
Paulo Moura