PLANO DE GESTÃO DE RISCOS

Relatório de avaliação intercalar

2023

Gabinete de Auditoria, Qualidade e Gestão do Risco
Setor de Gestão de Risco

SEGURANÇA SOCIAL

INSTITUTO DA SEGURANÇA SOCIAL, I.P.

Índice

Glossário

Siglas e Acrónimos	Descrição
AG	Autoridade de Gestão
Arachne	Ferramenta integrada de TI para extração e enriquecimento de dados disponibilizada pela Comissão, com o objetivo de apoiar as autoridades nacionais nos seus controlos administrativos e, bem assim, nas auditorias, assim prosseguindo e garantindo uma adequada proteção dos interesses financeiros da UE.
BD	Beneficiário direto - entidade responsável pela execução física e financeira das reformas e investimentos a financiar e que respondem diretamente pelos correspondentes marcos e metas estabelecidos no PRR
BF	Beneficiário final - a entidade responsável pela implementação e execução física e financeira de uma reforma e ou de um investimento, beneficiando de um financiamento do PRR diretamente enquanto «beneficiário direto», ou através do apoio de um «beneficiário intermediário»
BI	Beneficiário intermediário – entidade globalmente responsável pela execução das reformas e investimentos a financiar e pelos correspondentes marcos e metas estabelecidos no PRR, que selecionam entidades terceiras (beneficiário final) que se responsabilizam pela execução dos investimentos e das metas com elas contratualizadas
CD	Conselho Diretivo do ISS, I.P.
CNP	Centro Nacional de Pensões
DAP	Departamento de Administração do Património
DCGC	Departamento de Comunicação e Gestão do Cliente
DDS	Departamento de Desenvolvimento Social
DF	Departamento de Fiscalização
DGCF	Departamento de Gestão e Controlo Financeiro
DPC	Departamento de Prestações e Contribuições
DPRP	Departamento de Proteção Contra os Riscos Profissionais
DRH	Departamento de Recursos Humanos
EPD	Encarregado de Proteção de Dados
GAGI	Gabinete de Análise e Gestão da Informação
GAJC	Gabinete de Assuntos Jurídicos e Contencioso
GAQGR	Gabinete de Auditoria, Qualidade e Gestão de Risco
GPE	Gabinete de Planeamento e Estratégia
IP	Impacto
ISS, I.P.	Instituto de Segurança Social I.P.
MENAC	Mecanismo Nacional Anticorrupção
PGR	Plano de Gestão de Riscos, incluindo Riscos de Corrupção e Infrações Conexas
PO	Probabilidade
PO APMC	Programa Operacional de Apoio às Pessoas mais carenciadas
PO CH	Programa Operacional Capital Humano
PO ISE	Programa Operacional Inclusão Social e Emprego
PPDP	Privacidade e Proteção de Dados Pessoais
PRR	Plano de Recuperação e Resiliência
RGPC	Regime Geral da Prevenção da Corrupção
RGPD	Regulamento Geral de Proteção de Dados
UAP	Unidade de Apoio a Programas
UCE	Unidade de Contribuintes Estratégicos
UCI	Unidade de Coordenação Internacional
UGARNCCI	Unidade de Gestão e Acompanhamento da Rede Nacional de Cuidados Continuados Integrados
UTAE	Unidade Técnica de Arquitetura e Engenharia

1. Enquadramento

Em cumprimento do disposto no art.º 6.º, n.º 4, al. a), o relatório de avaliação intercalar do Plano de Gestão de Riscos (adiante designado PGR), que inclui o risco de corrupção e de infrações conexas, ocorre durante o mês de outubro.

O documento em apreço reflete a análise e avaliação realizada aos dados e indicadores recolhidos e disponibilizados pelas áreas para o efeito, no 1. º semestre de 2023, tendo como objetivos:

- A avaliação dos riscos macro, nomeadamente: risco tecnológico (dimensão estratégica e operacional) e risco de recursos humanos, de fraude (interna e externa) e violação de dados pessoais (na dimensão operacional);
- A avaliação da implementação das medidas preventivas de controlo face aos riscos identificados, por área funcional.

2. Avaliação dos riscos priorizados

2.1. Risco Operacional de Recursos Humanos e Pessoas

Na dimensão do risco operacional de recursos humanos são analisados e avaliados os seguintes riscos de categoria de risco nível 2:

a. Risco de Qualificação
b. Risco de Erro não Intencional
c. Risco de Quantidade
d. Risco de Clima Organizacional
e. Risco de Perda de Conhecimento

a. Risco de Qualificação

Risco de Qualificação	
Evento	Desajuste das competências/qualificações face às exigências das operações
Fatores de risco	Necessidades de Formação Capacidade produtiva
Fontes	DRH Balanço Social Indicadores de Gestão

Avaliação de risco:

Por comparação com o período homólogo, verifica-se um ligeiro aumento do risco de qualificação: avaliação anterior (1.º semestre 2022 – 4.15).

Risco de Qualificação

Manter Avaliação

Em face do resultado da avaliação do 1.º semestre de 2023, resulta: um nível de risco médio, com impacto moderado no cumprimento dos objetivos estratégicos e alguns requisitos de negócio em incumprimento, no que se refere à vertente operacional.

Proposta de ações a desenvolver:

- Devem ser identificadas pelas áreas operacionais as medidas adequadas para o tratamento do risco e planeada a sua implementação, com o objetivo de reduzir o risco a um nível aceitável;
- Manter avaliação da efetividade das medidas de controlo previstas para mitigação do risco.

b. Risco de Erro não Intencional

Risco de Erro não Intencional	
Evento	Erros na execução de operações por indefinição de procedimentos
Fator de risco	Erro nas decisões
Fonte	GAJC

Avaliação de risco:

Por comparação com o período homólogo, verifica-se um aumento do risco de erro não intencional: avaliação anterior (1.º semestre 2022 – 1.0).

Em face do resultado da avaliação do 1.º semestre de 2023, resulta: um nível de risco médio/baixo, com impacto moderado no cumprimento dos objetivos estratégicos e alguns requisitos de negócio em incumprimento, no que se refere à vertente operacional.

Proposta de ações a desenvolver:

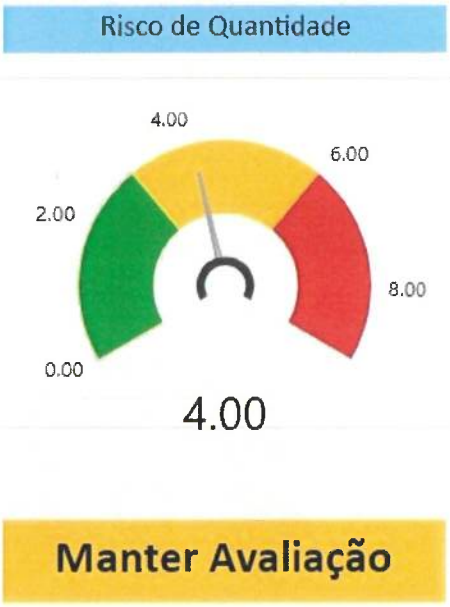
- Considerando a fronteira da avaliação baixo/médio, devem ser identificadas pelas áreas operacionais as medidas adequadas para o tratamento do risco e planeada a sua implementação, com o objetivo de reduzir o risco a um nível aceitável;
- Manter avaliação da efetividade das medidas de controlo previstas para mitigação do risco.

c. Risco de Quantidade

Risco de Quantidade	
Evento	Insuficiência de recursos humanos para realização das operações
Fatores de risco	Necessidades RH Trabalho extraordinário
Fontes	DRH Balanço Social Indicadores de Gestão

Avaliação de risco:

Por comparação com o resultado da avaliação anual (2022) verifica-se um ligeiro aumento (avaliação anual 2022 – 2.35).



Em face do resultado da avaliação do 1.º semestre de 2023, resulta: um nível de risco médio, com impacto moderado no cumprimento dos objetivos estratégicos e alguns requisitos de negócio em incumprimento, no que se refere à vertente operacional.
Para a presente avaliação contribuiu o facto de a taxa de reposição ser inferior aos anos 2022 e 2021, anos em que ocorreram muitas admissões de trabalhadores por via de procedimentos concursais concluídos.

Proposta de ações a desenvolver:

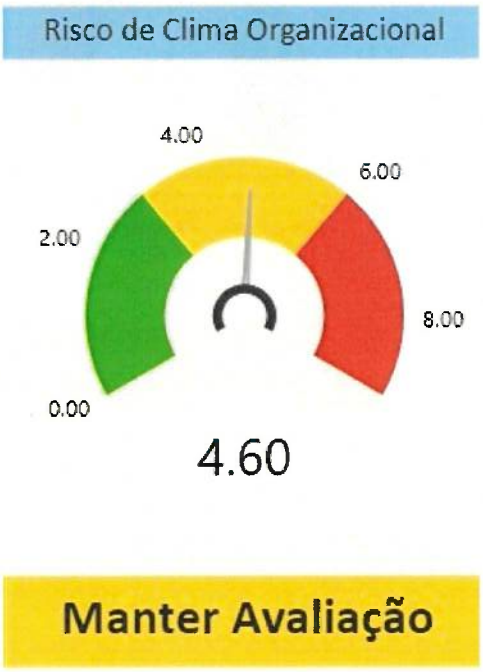
- Devem ser identificadas pelas áreas operacionais as medidas adequadas para o tratamento do risco e planeada a sua implementação, com o objetivo de reduzir o risco a um nível aceitável;
- Manter avaliação da efetividade das medidas de controlo previstas para mitigação do risco.

d. Risco de Clima Organizacional

Risco de Clima Organizacional	
Evento	Conflito/mau relacionamento interpessoal
Fatores de risco	Saída por Iniciativa do Trabalhador Comportamento disciplinar Colaboradores não satisfeitos/fraco envolvimento Ausências/faltas do trabalhador
Fontes	DRH Balanço Social Indicadores de Gestão

Avaliação de risco:

Por comparação com o período homólogo, verifica-se um ligeiro aumento do risco de clima organizacional: avaliação anterior (1.º semestre 2022 – 3.65).



Ainda não estão disponíveis alguns dados referentes a 2023, designadamente os resultados dos inquéritos de satisfação dos trabalhadores. Face a este constrangimento, o resultado da avaliação, resulta: num nível de risco médio, com impacto moderado no cumprimento dos objetivos estratégicos e alguns requisitos de negócio em incumprimento, no que se refere à vertente operacional.

Proposta de ações a desenvolver:

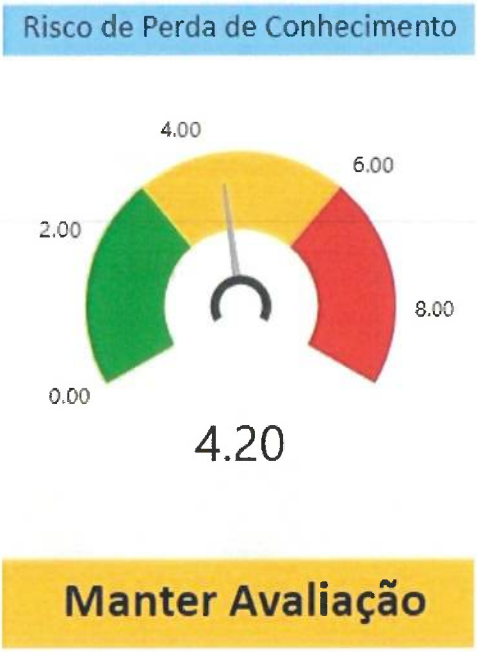
- Devem ser identificadas pelas áreas operacionais as medidas adequadas para o tratamento do risco e planeada a sua implementação, com o objetivo de reduzir o risco a um nível aceitável;
- Manter avaliação da efetividade das medidas de controlo previstas para mitigação do risco.

e. Risco de Perda de Conhecimento

Risco de perda de conhecimento	
Evento	Perdas por saídas de colaboradores
Fatores de risco	Rotatividade/turnover Envelhecimento dos quadros
Fonte	DRH Balanço Social

Avaliação de risco:

Por comparação com o período homólogo, verifica-se um aumento do risco de perda de conhecimento: avaliação anterior (1.º semestre 2022 – 3.00).



Em face do resultado da avaliação do 1.º semestre de 2023, resulta: um nível de risco médio, com impacto moderado no cumprimento dos objetivos estratégicos e alguns requisitos de negócio em incumprimento, no que se refere à vertente operacional.

Proposta de ações a desenvolver:

- Devem ser identificadas pelas áreas operacionais as medidas adequadas para o tratamento do risco e planeada a sua implementação, com o objetivo de reduzir o risco a um nível aceitável;
- Manter avaliação da efetividade das medidas de controlo previstas para mitigação do risco.

2.2. Risco Operacional Tecnológico

Na dimensão do risco operacional tecnológico são analisados e avaliados os seguintes riscos de categoria de risco nível 2:

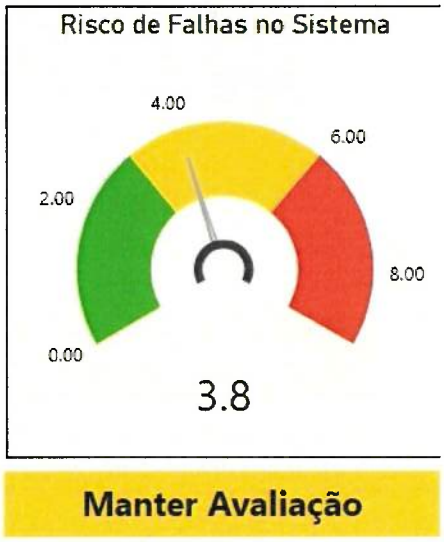
a. Risco de Falhas no Sistema
b. Riscos de Agilidade e Segurança da Informação
c. Riscos de Software

a. Risco de Falhas no Sistema

Risco de Falhas no Sistema	
Evento	Impossibilidade de continuidade dos processos decorrentes de erros ou falhas nos SI
Fatores de risco	Falhas nos SI (Sistemas de informação) Erros/desajustes SI
Fontes	GAGI II, IP

Avaliação de risco:

Por comparação com o período homólogo, verifica-se uma diminuição do risco de falhas no sistema: avaliação anterior (1.º semestre 2022 – 5.3).



Em face do resultado da avaliação do 1.º semestre de 2023, resulta: um nível de risco médio, com impacto moderado no cumprimento dos objetivos estratégicos e alguns requisitos de negócio em incumprimento, no que se refere à vertente operacional.

No 1.º semestre, verificou-se que as aplicações em que ocorreram maior n.º de falhas de sistema foram: PTSS, PTIN, RINA, justificando assim um maior acompanhamento em face do risco identificado.

Proposta de ações a desenvolver:

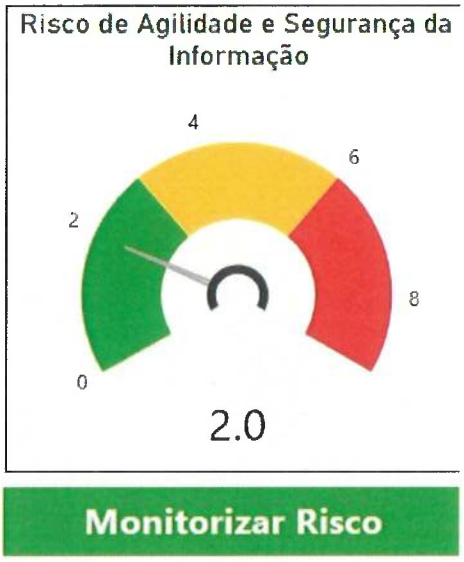
- Devem ser identificadas pelas áreas operacionais as medidas adequadas para o tratamento do risco e planeada a sua implementação, com o objetivo de reduzir o risco a um nível aceitável;
- Manter avaliação da efetividade das medidas de controlo previstas para mitigação do risco.

b. Risco de Agilidade e Segurança da Informação

Risco de Agilidade e Segurança da Informação	
Evento	Impossibilidade de receção, transmissão, armazenamento, processamento de informação em tempo útil e em segurança
Fator de risco	Acessos indevidos a informação
Fonte	GAQGR

Avaliação de risco:

Por comparação com o período homólogo, verifica-se a manutenção da avaliação do risco de agilidade e segurança da informação: avaliação anterior (1.º semestre 2022 – 2.0).



Ainda não estão disponíveis alguns dados referentes a 2023, designadamente a análise dos perfis de acesso ao SISS e os relatórios de auditoria interna, pelo que o nível de risco mantém-se baixo, ou seja, sem impacto no cumprimento dos objetivos estratégicos e nenhum requisito de Negócio afetado, no que se refere à vertente operacional.

Neste sentido, não se revela necessário a definição de medidas adicionais de controlo.

Proposta de ações a desenvolver:

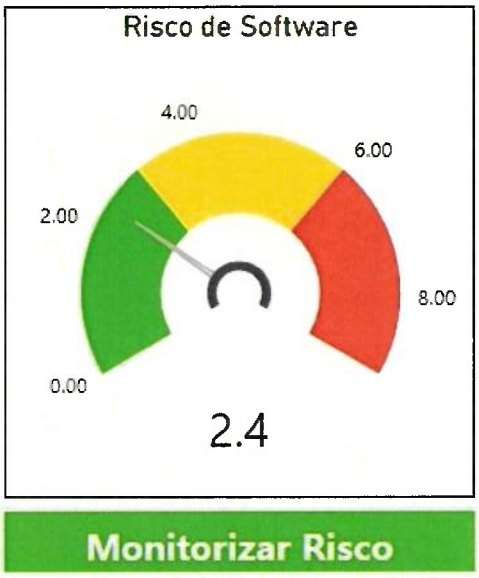
- Continuar a monitorizar o risco

c. Risco de Software

Risco de Software	
Evento	Falhas de segurança, conceção, falhas de integração entre os diversos sistemas, falhas de administração de sistemas, erros de programação, utilização inadequada de software, sistemas inadequados ou não padronizados para a organização, impossibilidade de integração entre os diversos sistemas, fragilidade no acesso, obsolescência.
Fator de risco	Obsolescência/desajuste
Fontes	GAGI II, IP

Avaliação de risco:

Por comparação com o período homólogo, verifica-se um ligeiro aumento do risco de Software: avaliação anterior (1.º semestre 2022 – 2.0).



Em face do resultado da avaliação do 1.º semestre de 2023, resulta: um nível de risco baixo, sem impacto no cumprimento dos objetivos estratégicos e nenhum requisito de Negócio afetado, no que se refere à vertente operacional.

Neste sentido, não se revela necessário a definição de medidas adicionais de controlo.

Proposta de ações a desenvolver:

- Continuar a monitorizar o risco

2.3. Risco operacional de fraude interna

Na dimensão do risco operacional de fraude interna são analisados e avaliados os seguintes riscos de categoria de risco nível 2:

a. Corrupção e Infrações Conexas

b. Apropriação Indevida
c. Outras Ações Fraudulentas

Na avaliação do risco de fraude interna, para além do cruzamento de indicadores e análise de dados de diferente natureza, foi tida em conta a existência de medidas de controlo preventivas e detetivas implementadas no âmbito da vigência do PGR.

Ao nível dos controlos detetivos implementados no Instituto, temos as ações de auditoria internas e o canal de denúncias (interno/externo), em que se apurou que no 1.º semestre de 2023, das ações realizadas pela área de auditoria não foram detetadas inconformidades, passíveis de configurar situações fraude interna. No Canal de Denuncias do ISS, I. P. não foram apresentadas denúncias suscetíveis de configurar situações de fraude.

Pelo exposto e à data da realização do presente relatório, o risco operacional de fraude interna é considerado baixo, sem impacto no cumprimento dos objetivos estratégicos e nenhum requisito de negócio afetado, no que se refere à vertente operacional.

Neste sentido, não se revela necessário a definição de medidas adicionais de controlo.

Avaliação de risco:

Monitorizar Risco

Em face do resultado da avaliação do 1.º semestre de 2023, resulta: um nível de risco baixo, sem impacto no cumprimento dos objetivos estratégicos e nenhum requisito de Negócio afetado, no que se refere à vertente operacional.
Neste sentido, não se revela necessário a definição de medidas adicionais de controlo.

Proposta de ações a desenvolver:

- Continuar a monitorizar o risco

2.4. Risco Operacional de Fraude Externa

Na dimensão do risco operacional de fraude externa são analisados e avaliados os seguintes riscos de categoria de risco nível 2:

a. Evasão a obrigações contributivas
b. Acesso indevido a direitos

Em termos de avaliação à data de 30.10.2023, extraem-se os seguintes resultados:

a. Evasão a obrigações contributivas

Evasão a obrigações contributivas	
Eventos	Perdas por manipulação de informação; falsificação de documentos; falsas declarações; omissão de informação; aproveitamento de fragilidades. Contribuições não declaradas; Não entrega das quotizações retidas aos trabalhadores.
Fatores de risco	Inexistência/falhas nos mecanismos de controlo (irregularidades/dívida contributiva); Inexistência/falhas nos mecanismos de controlo (abuso de confiança); Inexistência/falhas nos mecanismos de controlo (irregularidades/ contraordenações); Eficácia processual de contraordenações.
Fontes	DF, GAJC, GAGI

Avaliação de risco:

Por comparação com o período homólogo, verifica-se uma ligeira diminuição do risco de evasão a obrigações contributivas: avaliação anterior (1.º semestre 2022 – 4.50).

Em face do resultado da avaliação do 1.º semestre de 2023, resulta: um nível de risco médio, com impacto moderado no cumprimento dos objetivos estratégicos e alguns requisitos de negócio em incumprimento, no que se refere à vertente operacional.

Proposta de ações a desenvolver:

- Devem ser identificadas pelas áreas operacionais as medidas adequadas para o tratamento do risco e planeada a sua implementação, com o objetivo de reduzir o risco a um nível aceitável;
- Manter avaliação da efetividade das medidas de controlo previstas para mitigação do risco.

b. Acesso indevido a direitos

Acesso indevido a direitos	
Eventos	Manipulação de informação; falsificação de documentos; falsas declarações; omissão de informação; aproveitamento de fragilidades. Manipulações contributivas com vista ao acesso a direitos; baseadas numa relação de trabalho inexistente ou com referência a remunerações superiores às efetivamente auferidas, com intuito construção de carreira contributiva que permita o recebimento posterior de prestações sociais total ou parcialmente indevidas.
Fatores de risco	Inexistência/desajuste de acompanhamento Inexistência/falhas nos mecanismos de controlo Inexistência/falhas nos mecanismos de controlo (Burla) .
Fontes	DF, GAJC, GAGI

Avaliação de risco:

Por comparação com o período homólogo, verifica-se a manutenção do nível de risco de acesso indevido a direitos: avaliação anterior (1.º semestre 2022 – 4.80).

Em face do resultado da avaliação do 1.º semestre de 2023, resulta: um nível de risco médio, com impacto moderado no cumprimento dos objetivos estratégicos e alguns requisitos de negócio em incumprimento, no que se refere à vertente operacional.

Proposta de ações a desenvolver:

- Devem ser identificadas pelas áreas operacionais as medidas adequadas para o tratamento do risco e planeada a sua implementação, com o objetivo de reduzir o risco a um nível aceitável;
- Manter avaliação da efetividade das medidas de controlo previstas para mitigação do risco.

2.5. Risco Operacional de Violação de Dados Pessoais

Na dimensão de risco operacional de violação de dados pessoais são analisados e avaliados os seguintes riscos categoria nível 2:

a. Violação da Confidencialidade

b. Violação da Integridade (até à data da realização do presente relatório não existiam dados disponíveis para análise e avaliação deste risco)

c. Violação da Disponibilidade (até à data da realização do presente relatório não existiam dados disponíveis para análise e avaliação deste risco)

a. Violação da Confidencialidade

Violação da Confidencialidade	
Evento	Perdas decorrentes de situação em que existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais
Fator de risco	Insuficiência/desajuste dos mecanismos de controlo
Fonte	EPD/II

Avaliação de risco:

Por comparação com o período homólogo, verifica-se um ligeiro aumento do risco de violação de confidencialidade: avaliação anterior (1.º semestre 2022 – 1.0).

Em face do resultado da avaliação do 1.º semestre de 2023, resulta: um nível de risco baixo, sem impacto no cumprimento dos objetivos estratégicos e nenhum requisito de Negócio afetado, no que se refere à vertente operacional.
Neste sentido, não se revela necessário a definição de medidas adicionais de controlo.

Proposta de ações a desenvolver:

- Continuar a monitorizar o risco

b. Violação da Integridade

Violação da Integridade	
Evento	Perdas por alteração acidental ou não autorizada dos dados pessoais
Fator de risco	Insuficiência/desajuste dos mecanismos de controlo
Fonte	EPD/II

Nota: Até à data da realização do presente relatório não existiam dados disponíveis para análise e avaliação dos riscos de violação de integridade.

c. Violação da Disponibilidade

Violação da Disponibilidade	
Evento	Perdas de acesso ou a destruição acidental ou não autorizada de dados pessoais
Fator de risco	Insuficiência/desajuste dos mecanismos de controlo
Fonte	EPD/II

Nota: Até à data da realização do presente relatório não existiam dados disponíveis para análise e avaliação dos riscos de violação da disponibilidade.

3. Avaliação de medidas previstas por área funcional

O PGR envolve 20 áreas funcionais do ISS, I.P, nas quais foram identificados 133 eventos de risco e previstas 178 medidas de mitigação específicas, conforme tabela seguinte:

Tabela 1 – Áreas, riscos e medidas

Áreas Funcionais	Riscos	Medidas Específicas
DAP	9	16
GAGI	3	7
UAP	21	51
UTAE	3	4
GAJC	5	6
GAQGR	6	8
DCGC	4	4
DPC	11	17
UCE	2	4
UCI	4	1
UGARNCCI	1	5
DDS	19	8
DF	5	5
CD	6	3
DGCF	7	7
GPE	8	10
CNP	4	4
PPDP	4	6
DPRP	2	3
DRH	9	9
20	133	178

Não obstante a informação intercalar, nos termos do art.º 6º, n.º 4, al. a) do DL n.º 109-E/2021, incidir sobre as situações identificadas com risco alto, entendeu-se iniciar a avaliação de todas as medidas identificadas, por se tratar de uma nova versão do PGR, fruto das revisões operadas no documento. Esta ação de avaliação do cumprimento das medidas de controlo continua em execução tendo data prevista de conclusão durante a vigência do PGR.

No 1.º semestre de 2023, foram verificadas 6 das 20 áreas de atuação do ISS, I.P. (DCGC, GAQGR, GPE, PPDP, UCI E UGARNCCI) tendo o resultado dessa análise permitido avaliar as medidas previstas quanto à sua implementação do seguinte modo:

- Implementado (I) – Medida de controlo implementada na totalidade

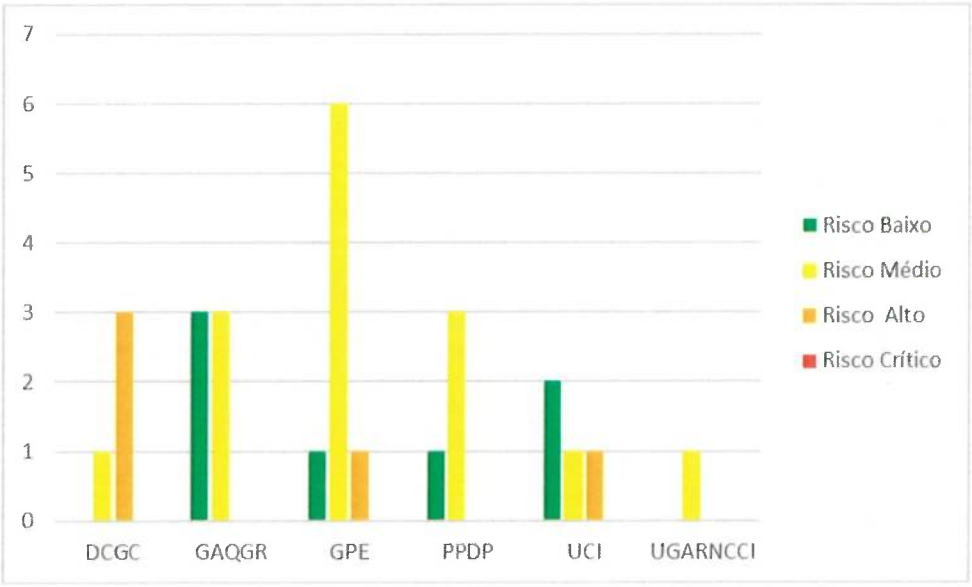
- Em Curso (EC) – Medida de controlo em que a implementação ainda não foi concluída
- Por Iniciar (PI) – Medida de controlo ainda não implementada

Nas áreas em avaliação, o PGR identifica um total de 27 eventos de risco (5 de risco alto, 15 de risco médio e 7 de risco baixo. Da aplicação da matriz, não resultou nenhum risco identificado como crítico (cf. Tabela 2):

Tabela 2 – Áreas analisadas vs. níveis de risco

Áreas Funcionais	Risco Baixo	Risco Médio	Risco Alto	Risco Crítico
DCGC	0	1	3	0
GAQGR	3	3	0	0
GPE	1	6	1	0
PPDP	1	3	0	0
UCI	2	1	1	0
UGARNCCI	0	1	0	0
Total Geral	**7**	**15**	**5**	**0**

Gráfico 1 – Níveis de risco por área analisada



Para mitigar os riscos identificados, encontram-se previstas 39 medidas de controlo. Da avaliação realizada, verifica-se que as medidas de controlo apresentam diferentes estados de implementação: 72% implementadas, 20% em curso e 3% por iniciar.

Tabela 3 – Estado de Implementação das medidas por área

Áreas	Medidas específicas	Estado de Implementação			
		Imp.	Em curso	Por iniciar	n.a.
GAQGR	8	75%	25%	0%	0%
DCGC	4	0%	100%	0%	0%
UCI	1	100%	0%	0%	0%
UGARNCCI	5	80%	20%	0%	0%
GPE	15	80%	7%	7%	6%
PPDP	6	83%	0%	0%	17%
Totais:	39	72%	20%	3%	5%

Em concreto, a avaliação específica por área encontra-se em anexo (I) ao presente relatório.

Para além das medidas especificas, por área funcional, também as medidas de controlo transversal foram objeto de avaliação:

Tabela 4 – Estado de implementação das medidas de controlo transversal

	Medidas transversais previstas	Resultado da verificação	Estado
1	Estratégia antifraude	Revisão efetuada em janeiro de 2023. Publicada	Implementado
2	Código de Ética e Conduta do ISS, I.P., inclui política de conflito de interesses	Revisão em janeiro de 2023. Publicado	Implementado
3	Subscrição de declarações de aceitação do Código de Ética e Conduta;	Última subscrição: 2022	Implementado
4	Declarações de inexistência de conflitos de interesses	Última subscrição: 2021/22 (transversal a todos os trabalhadores do ISS, I.P.). Subscrições específicas 2023: Contratação pública – subscrição de DICI por processo de acordo com o modelo do CCP; PRR – subscrição de DICI na aplicação de suporte, por candidatura e por técnico que intervém em cada fase.	Implementado parcialmente
5	Divulgação interna e externa (Intranet e Internet): Missão, Visão, Valores, Plano de Gestão de Riscos entre outros documentos/informação;	Intranet e internet do ISS, I.P.	Implementado
6	Plano de Gestão de Riscos (inclui corrupção e infrações conexas)	Revisão realizada em janeiro de 2023.	Implementado
7	Ações de sensibilização a todos os trabalhadores: temas abordados: Ética, Conduta, Conflito de Interesses, Prevenção de Riscos (incluindo divulgação do PGR e prevenção da Fraude), Proteção de Dados Pessoais	Conforme Plano de formação em vigor para 2023 - 3 sessões realizadas em 2023	Implementado
8	Instrumento de reporte/tratamento de denúncias – Candal da Denúncia	Novo Canal da Denúncia, em vigor desde fevereiro de 2023, disponível na Internet e Intranet (canal externo e interno)	Implementado
9	Manuais de Processos, procedimentos definidos, orientações técnicas	Disponíveis da Intranet do ISS, I. P.	Implementado
10	Acompanhamento de indicadores de gestão/atividades funcionais	Disponíveis em diversos instrumentos	Implementado

11	Segregação de funções	Verificação em sede de auditoria interna (AI)	Implementado
12	Rotatividade de equipas (qd possível/aplicável)	Verificação em sede de auditoria interna (AI)	Implementado
13	Procedimentos conferência/autorização por 2.ª pessoa (qd aplicável)	Verificação em sede de auditoria interna (AI)	Implementado
14	Modelo de avaliação do risco e estrutura de responsabilidades	Definido no Manual do Processo de Gestão de Risco, articulado com o Plano de Gestão de Riscos	Implementado
15	Política de acesso ao sistema de informação	Política definida; controlo em sede de AI	Implementado
16	Delegações e subdelegações de competências	Verificação em sede de auditoria interna (AI)	Implementado
17	Sistema de informação de suporte às atividades	Ainda não cobre a totalidade das atividades	Implementado parcialmente
18	Auditorias internas	Plano anual aprovado pelo CD do ISS, I. P	Implementado
19	Procedimentos de conferência/validação por 2.ª pessoa	Verificação em sede de auditoria interna (AI)	Implementado

Verifica-se que a quase totalidade das medidas transversais previstas se encontram implementadas, existindo duas medidas (Sistema de informação de suporte às atividades e Declarações relativas a conflito de interesses) implementadas parcialmente, uma vez que:

- O sistema de informação ainda não abrange a totalidade das áreas;
- Aguarda-se a minuta a disponibilizar para o efeito, nos termos legalmente previstos, com exceção dos trabalhadores afetos ao PRR, que assinalam aplicacionalmente a inexistência de situação de conflito de interesses e os trabalhadores afetos à contratação pública.

4. Conclusões

Ao nível da avaliação dos riscos priorizados do PGR, por comparação com o mesmo período homólogo (1.º semestre 2022), obteve-se a seguinte avaliação de risco:

- Riscos operacionais de recursos humanos e pessoais sofreram um ligeiro aumento;
- Riscos operacionais tecnológicos verifica-se que, o risco de falhas de sistemas diminuiu, o risco de agilidade e segurança da informação mantém a mesma avaliação e o risco de software sofreu um ligeiro aumento;
- Riscos de fraude interna, não foram detetadas novas situações suscetíveis de configurar risco de fraude interna, pelo que a avaliação de risco se mantém de nível baixo;
- Riscos de fraude externa, verifica-se uma ligeira diminuição da avaliação do risco de evasão a obrigações contributivas e a manutenção da avaliação do risco de acesso indevido a direitos, com base nos dados disponibilizados pelas áreas até ao momento;

- Riscos de violação de dados pessoais verifica-se um ligeiro aumento, no entanto o nível de risco mantém-se baixo devendo manter-se a avaliação da efetividade dos controlos de risco existentes.

Relativamente à avaliação de implementação das medidas de mitigação por área, das áreas já avaliadas verifica-se uma taxa de implementação de 72%, perspetivando-se que a taxa aumente até final do ano de 2023, por existirem três áreas (GAQGR, DCGC, GPE) que apresentam medidas de controlo com o estado de implementação em curso.

A avaliação e monitorização do PGR continuará a ser realizada no 2.º semestre de 2023, permitindo a elaboração do relatório anual no mês de abril de 2024, conforme prevê o RGPC.

5. Anexos

5.1 Anexo I – Grelhas de monitorização das medidas de mitigação específicas por área

Gabinete de Planeamento e Estratégia (GPE)								Responsável: Direção
Principais Atividades	Eventos de Risco	PO	IP	Nível de Risco	Medidas	Verificação	Estado de Implementação	Observações
Análise e seleção de candidaturas a programas nacionais e comunitários, nomeadamente os programas delegados pela AG; Verificações de gestão.	Análise incorreta intencional	2	3	6	Avisos de abertura de candidaturas devidamente publicitados	✓	Imp.	
					Utilização de Checklist de procedimentos	✓	EC	A área informa que estão a ser desenhados manuais de procedimentos, não disponibiliza calendarização.
					Todas as candidaturas registadas e sujeitas a critérios de avaliação e seleção conforme os procedimentos definidos e aprovados	✓	Imp.	
					Todas as decisões comunicadas aos candidatos	✓	Imp.	
					Política de gestão de acessos ao sistema de informação	✓	Imp.	
					Sistema de informação de suporte às atividades	✓	Imp.	
					Procedimentos de conferência/validação por 2.ª pessoa	✓	Imp.	
	Conflitos interesse entre trabalhadores do GPE e candidatos ou beneficiários.	2	2	4	Subscrição de declarações de inexistência de conflito de interesses	✓	Imp.	
					Rotatividade	✓	Imp.	
					Delegações e subdelegações de competências	✓	Imp.	
					Segregação de funções	✓	Imp.	
	Falsas declarações prestadas pelos candidatos ou beneficiários.	2	2	4	É adotada uma metodologia para efeito da realização das verificações de gestão que contempla uma análise de risco de fraude	×	PI	A área não disponibilizou informação de calendarização de implementação desta medida.
	Duplo financiamento	2	2	4	Cruzamento de informação com as autoridades nacionais que administram os fundos	✓	Imp.	
	Processo de verificação de gestão incompleto ou desadequado	1	2	2	Ações de acompanhamento no local realizadas por 2.º pessoa	n.a	n.a	Medida de controlo cuja competência de implementação é de outra área, por segregação de funções.
					Segregação de funções	✓	Imp.	
					Determinar, no âmbito dos programas de investimento, os montantes de investimento de cada componente por fonte de financiamento e proceder à hierarquização dos projetos, de acordo com o modelo definido para cada programa	✓	Imp.	

Privacidade e Proteção de Dados Pessoais (PPDP)								Responsável: EPD
Principais Atividades	**Eventos de Risco**	**PO**	**IP**	**Nível de Risco**	**Medidas**	**Verificação**	**Estado de Implementação**	**Observações**
Transversal a todas as atividades do ISS, I.P.	Uso indevido de dados pessoais / confidenciais por: divulgação a terceiros não legitimados; eventual utilização em proveito próprio	1	3	3	Controlo de acessos a sistemas de informação	✓	Imp.	
	Perdas decorrentes de situação em que existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais	1	3	3	Segurança de recursos humanos	✓	Imp.	
	Perdas por alteração ou destruição acidental ou não autorizada dos dados pessoais	2	2	4	Segurança de acessos físicos	✓	Imp.	
					Organização da segurança da informação	✓	Imp.	
					Segurança nas comunicações	✓	Imp.	
	Indisponibilidade de acesso às aplicações.	1	2	2	Política de segurança	n.a.	n.a.	Na ação de conformidade verificou-se que a implementação desta medida de controlo é de outra área.

Legenda:

Probabilidade de Ocorrência (PO): 1 - Baixa; 2 - Média; 3 - Alta

Impacto (IP) (Gravidade da Consequência): 1 - Baixo; 2 - Médio; 3 - Alto

Nível de Risco: B - Baixo (1,2); M - Médio (3,4); A - Alto (6); C - Crítico (9)

Estado de Implementação: Imp.- Implementado(I); Em curso (EC); Por iniciar (PI)

Comunicação e Gestão do Cliente (DCGC)							Responsável: Direção	
Principais Atividades	Eventos de Risco	PO	IP	Nível de Risco	Medidas	Verificação	Estado de Implementação	Observações
Realizar atendimentos.	Alteração, intencional ou não, de dados pessoais do cliente (beneficiário ou contribuinte).	2	2	4	Controlo aleatório da conformidade dos movimentos efetuados pelos utilizadores do SI de suporte	✓	EC	Resultado da verificação de implementação em 19 serviços: Medida de controlo implementada em 11, 3 em curso e 5 por iniciar.
Registar NIB e morada.	Apropriação indevida de valores por registos de NIB que não os do cliente (beneficiário ou contribuinte).	3	2	6	Rotatividade de RH nos serviços de atendimento	✓	EC	Resultado da verificação de implementação em 19 serviços: Medida de controlo implementada em 16 serviços, 2 em curso e 1 por iniciar.
Controlar o acesso e utilização dos perfis informáticos.	Apropriação indevida de valores por registos de moradas que não as do cliente (beneficiário ou contribuinte).	2	3	6	Confirmação pelo coordenador /chefe de equipa da alteração de moradas e alteração de NIB	✓	EC	Resultado da verificação de implementação em 19 serviços: Medida de controlo implementada em 18 serviços e 1 por iniciar.
	Acesso indevido às bases de dados utilizadas no Atendimento devido à atribuição de perfis sem controlo.	3	2	6	Controlo pela Coordenação dos perfis efetivamente atribuídos no Serviço de Atendimento	✓	EC	Resultado da verificação de implementação em 19 serviços: Medida de controlo implementada em 15 serviços, 2 em curso e 2 por iniciar.

Legenda:

Probabilidade de Ocorrência (PO): 1 - Baixa; 2 - Média; 3 - Alta

Impacto (IP) (Gravidade da Consequência): 1 - Baixo; 2 - Médio; 3 - Alto

Nível de Risco: B - Baixo (1,2); M - Médio (3,4); A - Alto (6); C - Crítico (9)

Estado de Implementação: Imp.- Implementado(I); Em curso (EC); Por iniciar (PI)

Auditoria, Qualidade e Gestão de Risco (GAQGR)								Responsável: Direção
Principais Atividades	**Eventos de Risco**	**PO**	**IP**	**Nível de Risco**	**Medidas**	**Verificação**	**Estado de Implementação**	**Observações**
Análise e tratamento de dados e informação.	Utilização indevida de informação.	1	2	2	Limitação do âmbito e tempo, dos acessos aos suportes aplicacionais	✓	Imp.	
Realização de ações de controlo interno (auditoria, averiguação, outras).	Inadequação na aplicação de métodos e técnicas com o objetivo de favorecer e/ou omitir intencionalmente.	2	2	4	Rotatividade de equipas	✓	Imp.	
	Omissão intencionalmente informação relevante.	2	2	4	Plano Anual de Auditorias Internas do ISS, I.P.	✓	Imp.	
					Plano de Gestão de Riscos do ISS, I.P	✓	Imp.	
Acompanhamento da implementação das recomendações de ações de controlo interno e externo.	Não aplicação das políticas, normas, metodologias e procedimentos em vigor aplicáveis às ações de controlo e auditoria.	1	2	2	Acompanhamento e supervisão das atividades desenvolvidas, através de diversos níveis hierárquicos	✓	Imp.	
Processos a modelar e/ou atualizar	Desajuste de ferramentas informáticas face às necessidades.	3	1	3	Desenvolver a implementação da aplicação de Gestão de Processos, RGPD e Risco	✓	EC	Medida cuja implementação está em curso, prevendo-se a conclusão em dezembro de 2023
Avaliar o desempenho dos processos do ISS, I.P.	Ausência de informação centralizada e atualizada relativamente aos processos.	2	1	2	Garantir a realização das reuniões da Comissão de Gestão de Risco e de Processos (quando aplicável)	✓	Imp.	
					Definir e comunicar calendário de reporte dos dados dos indicadores e garantir a existência e manutenção de repositório de informação	✓	EC	Medida cuja implementação está em curso, prevendo-se a conclusão em dezembro de 2023

Legenda:

Probabilidade de Ocorrência (PO): 1 - Baixa; 2 - Média; 3 - Alta

Impacto (IP) (Gravidade da Consequência): 1 - Baixo; 2 - Médio; 3 - Alto

Nível de Risco: B - Baixo (1,2); M - Médio (3,4); A - Alto (6); C - Crítico (9)

Estado de Implementação: Imp.- Implementado(I); Em curso (EC); Por iniciar (PI)

Coordenação Internacional (UCI)							Responsável: Direção	
Principais Atividades	Eventos de Risco	PO	IP	Nível de Risco	Medidas	Verificação	Estado de Implementação	Observações
Pedido de prestação e reembolso com aplicação de instrumentos internacionais de desemprego.	Identificação/qualificação indevida; manipulação de dados; falsas declarações. constituição de carreira contributiva indevida.	2	2	4	Controlo aleatório de processos (documentação entregue)	✓	Imp.	
Pedido de prestação e reembolso com aplicação de instrumentos internacionais de doença.	Acesso indevido a direito.	2	3	6				
Determinação da Legislação Aplicável (e emissão de atestado de direito).	Erro e/ou omissão não intencional no registo de informação na aplicação de suporte.	2	1	2				
Cobrança de Contribuições EE Estrangeiras.	Identificação/qualificação indevida; falsas declarações.	2	1	2				

Legenda:

Probabilidade de Ocorrência (PO): 1 - Baixa; 2 - Média; 3 - Alta

Impacto (IP) (Gravidade da Consequência): 1 - Baixo; 2 - Médio; 3 - Alto

Nível de Risco: B - Baixo (1,2); M - Médio (3,4); A - Alto (6); C - Crítico (9)

Estado de Implementação: Imp.- Implementado(I); Em curso (EC); Por iniciar (PI)

Unidade de Cuidados Continuados (UGARNCCI)							Responsável: Direção	
Principais Atividades	**Eventos de Riscos**	**PO**	**IP**	**Nível de Risco**	**Medidas**	**Verificação**	**Estado de Implementação**	**Observações**
Gerir pedidos de comparticipação para cuidados continuados integrados	Atribuição de comparticipação indevida	2	2	4	Controlo dos pedidos através de conferência por 2.ª pessoa	✓	Imp.	
					Automatização máxima do processo de forma a diminuir o Risco de RH e o Risco de erro não intencional	✓	Imp.	
					Interoperabilidade dos sistemas de informação: Segurança Social/ AT/ Saúde- Sistema de Informação da RNCCI	✓	EC	
					Perfis de acesso à Informação controlados (existe e previne o Risco de violação de dados pessoais)	✓	Imp.	
					Recolha de Consentimento informado previa à utilização dos dados pessoais (existe e previne o Risco de violação de dados pessoais)	✓	Imp.	

Legenda:

Probabilidade de Ocorrência (PO): 1 - Baixa; 2 - Média; 3 - Alta

Impacto (IP) (Gravidade da Consequência): 1 - Baixo; 2 - Médio; 3 - Alto

Nível de Risco: B - Baixo (1,2); M - Médio (3,4); A - Alto (6); C - Crítico (9)

Estado de Implementação: Imp.- Implementado(I); Em curso (EC); Por iniciar (PI)