Plano de Gestão de Riscos do ISS, IP

SEGURANÇA SOCIAL

INSTITUTO DA SEGURANÇA SOCIAL, I.P.

FICHA TÉCNICA

TÍTULO	Plano de Gestão de Riscos do ISS, IP	
AUTOR	Núcleo de Qualidade e Gestão do Risco/GAQGR	
DATA APROVAÇÃO	2020-11-12	
EDIÇÃO	1.0	
PROPRIEDADE	Instituto da Segurança Social, I.P.	
CONTACTOS		Av. 5 de Outubro, n.º 175 1069-451 Lisboa
	@	ISS-GAQGR@seg-social.pt

Histórico de Alterações

[Inserir lista de alterações que dão origem a uma nova versão do documento]

Ed.	Data	Alteração	Validado	Data	Aprovação	Data
1.0	2020-10-21	Alteração dos indicadores associados ao Risco de Violação de Dados Pessoais/ Violação da disponibilidade Ajustamento na Estrutura da Gestão de Risco	CGR	2020-10-29	CD	2020-11-12

Índice

Índice de quadros e figuras

1. Enquadramento

A gestão de risco enquanto componente fundamental da gestão estratégica, apoia a tomada de decisão face a fenómenos cujos efeitos/impactos podem comprometer o desempenho da organização.

Os riscos associados ao exercício das diferentes atividades desenvolvidas pelo ISS, IP apresentam-se como fatores potenciadores de eventuais desvios de atuação, que importa obviar atempadamente através da implementação de medidas de natureza preventiva, destinadas a diminuir o efeito, positivo ou negativo, da incerteza provocada pelos mesmos (ISO 31000:2009 – Risk Management –Principles and guidelines).

A incorporação da gestão do risco no ISS, IP tem como objetivo estabelecer um conjunto de práticas de identificação, análise, avaliação, tratamento, revisão, monitorização e reporte dos principais riscos.

Até este momento, a prossecução da política de gestão de risco no ISS, IP foi assegurada através do Plano de Prevenção dos Riscos de Corrupção e Infrações Conexas, enquanto instrumento de gestão e controlo internos, elaborado em cumprimento da Recomendação do Conselho de Prevenção da Corrupção n.º 1/2009, de 1 de julho de 2009, que determinou:

> *"1.1 - Os órgãos dirigentes máximos das entidades gestoras de dinheiros, valores ou património públicos, seja qual for a sua natureza, devem, no prazo de 90 dias, elaborar planos de gestão de riscos de corrupção e infrações conexas, contendo, nomeadamente, os seguintes elementos:*
>
> *a) Identificação, relativamente a cada área ou departamento, dos riscos de corrupção e infrações conexas;*
>
> *b) Com base na referida identificação de riscos, indicação das medidas adotadas que previnam a sua ocorrência (por ex., mecanismos de controlo interno; segregação de funções, definição prévia de critérios gerais e abstratos, designadamente na concessão de benefícios públicos e no recurso a especialistas externos, nomeação de júris diferenciados para cada concurso, programação de ações de formação adequada, etc.);*
>
> *c) Definição e identificação dos vários responsáveis envolvidos na gestão do plano, sob a direção do órgão dirigente máximo;*
>
> *d) Elaboração anual de um relatório sobre a execução do plano.*
>
> *Os planos e os relatórios de execução referidos no número anterior devem ser remetidos ao Conselho de Prevenção da Corrupção, bem como aos órgãos de superintendência, tutela e controlo."*

Este Plano, elaborado pela primeira vez em 2010 e com revisões e atualizações periódicas, vigorou até 2019.

A Recomendação do Conselho de Prevenção da Corrupção de 1 de julho de 2015, determinou no seu n.º 1:

> *"1. Os Planos de Prevenção de Riscos de Corrupção e Infrações Conexas, objeto das Recomendações n.ºs 1/2019, de 1 de julho, e 1/2010, de 7 de abril, em resultados de um processo de análise e reflexão interna das entidades respetivas, devem identificar de modo exaustivo os riscos de gestão, incluindo os de corrupção, bem como as correspondentes medidas preventivas."*

Neste seguimento, o ISS, IP procedeu à definição do Sistema de Gestão do Risco, tendo sido aprovado em 2016 o Processo de Gestão do Risco, que estabelece a estrutura e metodologia a implementar na organização.

Em alinhamento com a Política de Gestão de Risco e a missão do ISS, IP, foram identificados todos os riscos a que organização se encontra exposta. A identificação de riscos no ISS, IP foi desenvolvida de forma metódica, garantindo que todas as atividades significativas da organização fossem consideradas e que todos os riscos decorrentes fossem refletidos.

Esta fase envolveu a pesquisa de referenciais de boas práticas e a auscultação da perceção dos dirigentes das unidades orgânicas centrais, tendo resultado na sistematização de um catálogo que estrutura os riscos por dimensões (operacional e estratégica), classificados por categorias de Nível 1 e 2, numa lógica de desdobramento.

A análise dos riscos identificados pressupôs a definição de uma ferramenta que permitisse determinar a magnitude de um risco, expressa em termos da combinação das consequências / impacto e das suas probabilidades de ocorrência na organização.

A Matriz de Avaliação de Riscos do ISS, IP, constitui a base para determinar o nível de risco e as ações para o respetivo tratamento (Fig. 10 – Matriz de Avaliação de Risco). Partindo das categorias de riscos previamente identificadas e aplicando esta matriz, foi realizada uma análise qualitativa através da aplicação de um questionário de perceção quanto à probabilidade de ocorrência e impactos dos riscos a que o ISS, IP se encontra exposto. A análise dos resultados destes questionários permitiu priorizar as categorias de riscos a avaliar e tratar.

Nesta sequência, pretende-se agora dar continuidade ao processo iniciado com o PPRIC, com a elaboração do presente Plano de Gestão de Riscos do ISS, IP que visa promover a compreensão sobre a natureza dos riscos priorizados, eventos de risco, fatores e indicadores-chave, constituindo um input importante para a fase de avaliação de riscos e para as decisões sobre a necessidade de os mesmos serem tratados, as estratégias e métodos mais adequados.

2. Caracterização do ISS, IP

O Instituto da Segurança Social, I.P. (ISS, IP) é um instituto público integrado na administração indireta do Estado, dotado de autonomia administrativa e financeira, com personalidade jurídica, património próprio e jurisdição sobre todo o território nacional (sem prejuízo das atribuições e competências das Regiões Autónomas dos Açores e Madeira).

A estrutura orgânica compreende:

- Serviços Centrais,
- Centros Distritais, e
- Centro Nacional de Pensões

Os Serviços estão organizados em Áreas Operacionais, de Administração Geral e de Apoio Especializado.

2.1. Missão, Visão e Valores

Quadro 1 – Missão, Visão e Valores

Missão	**Garantir a proteção e a inclusão social das pessoas, reconhecendo os seus direitos, assegurando o cumprimento das obrigações contributivas e promovendo a solidariedade social.**
Visão	Ser o elo de confiança da sociedade portuguesa na coesão social, promovendo um serviço humanista, de proximidade e de excelência.
Valores	**Humanismo** Valorizamos as pessoas. **Ética** Agimos com integridade. **Confiança** Geramos confiança. **Respeito** Respeitamos a diversidade. **Solidariedade** Somos solidários.

2.2. Atribuições e cadeia de valor

O ISS, IP prossegue atribuições do Ministério do Trabalho, Solidariedade e Segurança Social (MTSS) sob superintendência e tutela do respetivo Ministro:

- Gere os regimes de segurança social, incluindo o tratamento, recuperação e reparação de doenças ou incapacidades resultantes de riscos profissionais,
- Reconhece os direitos e o cumprimento das obrigações decorrentes dos regimes de segurança social e demais subsistemas da segurança social, incluindo o exercício da ação social, e
- Assegura a aplicação dos acordos internacionais no âmbito do sistema da segurança social.

Para o efeito, desenvolve um conjunto de atividades com vista a garantir valor acrescentado aos seus clientes e partes interessadas. Estas atividades estruturam-se em macroprocessos que são detalhados ou desdobrados para os níveis tático e operacional.

Os macroprocessos encontram-se identificados na Cadeia de Valor aprovada pelo Conselho Diretivo, representada na figura seguinte.

Figura 1 – Cadeia de Valor do ISS, IP

2.3. Estrutura orgânica

A estrutura orgânica do Instituto compreende os Serviços Centrais, 18 serviços desconcentrados (os Centros Distritais) e o Centro Nacional de Pensões.

Figura 2 – Organigrama do Instituto da Segurança Social, IP

Os Centros Distritais do ISS, IP refletem realidades distritais diversas em dimensão e complexidade, que se traduzem numa estrutura orgânica diferenciada. No entanto, procurando um equilíbrio entre estas diversas

realidades com vista à harmonização possível da estrutura dos serviços, identificam-se quatro grupos de centros distritais, definidos em função do número de beneficiários abrangidos.

Dentro de cada grupo foi estabelecida, em articulação com os respetivos Diretores de Segurança Social (DSS), uma estrutura de unidades e núcleos comum, que posteriormente foi ajustada à realidade concreta de cada distrito com a criação de setores e equipas.

Quadro 2 - Tipologias de Centros Distritais

Tipologia	Beneficiários ativos	Centros Distritais
1	Mais de 800.000	Lisboa e Porto
2	Mais de 300.000 e menos de 800.000	Aveiro, Braga e Setúbal
3	Mais de 100.000 e menos de 300.000	Coimbra, Faro, Leiria, Santarém e Viseu
4	Menos de 100.000	Beja, Bragança, Castelo Branco, Évora, Guarda, Portalegre, Viana do Castelo e Vila Real

Fonte: Relatório de Atividades ISS, IP

Os Centros Distritais integram ainda os Estabelecimentos Integrados e os Serviços Locais.

Os Serviços Centrais estão organizados em áreas operacionais, de administração geral, que assumem a natureza de serviços comuns a toda a estrutura do ISS, IP, e de apoio especializado, com a seguinte distribuição.

Figura 3 – Organização dos Serviços Centrais do ISS, IP

Fonte: Relatório de Atividades do ISS, IP

Os Departamentos e Gabinetes do ISS, IP organizam-se em Unidades e Núcleos a constituir mediante deliberação do Conselho Diretivo. Podendo ainda estruturar-se em setores e equipas, igualmente a constituir por deliberação do Conselho Diretivo.

2.4. Recursos Humanos e Financeiros

Quadro 3 – Estrutura dos Recursos Humanos do ISS, IP

	2020	2019	2018	2017	2016
ISS, IP (Dados a 31.dez do ano anterior)	8.195	7.860	7.600	7.562	7.318
Masculino	1.363	1.346	1.336	1.326	1.322
Feminino	6.832	6.514	6.264	6.236	5.996

Fonte: PAISS 2020

Quadro 4 – Estrutura dos Recursos Financeiros do ISS, IP

	2020	2019	2018	2017	2016
ISS, IP	24.596,23	23.889,82	23.222,40	22.269,14	22.081,24
Sistema de Proteção Social de Cidadania	7.267,21	7.088,33	6.940,20	6.942,02	6.910,61
Ação Social	1.653,83	1.642,38	1.575,00	1.540,84	1.514,48
Solidariedade	4.032.17	3.969,40	3.977,30	4.279,63	4.270,64
Proteção Familiar	1.581,20	1.476,55	1.387,80	1.121,55	1.125,49
Sistema Previdencial (Inclui Regimes Especiais)	17.077,40	16.555,77	15.756,50	15.112,63	14.956,91
Administração	251,62	245,72	225,8	214,49	213,72

Fonte: PAISS 2020

3. Gestão Estratégia da gestão de risco no ISS, IP

A gestão de risco enquanto instrumento de gestão e controlo interno, assegura a prossecução da Política de Gestão de Risco do ISS, I.P na otimização da capacidade de alcançar os objetivos e prioridades estratégicas constantes do Plano Estratégico do ISS, IP, bem como, minimizar o impacto potencial dos riscos nos resultados.

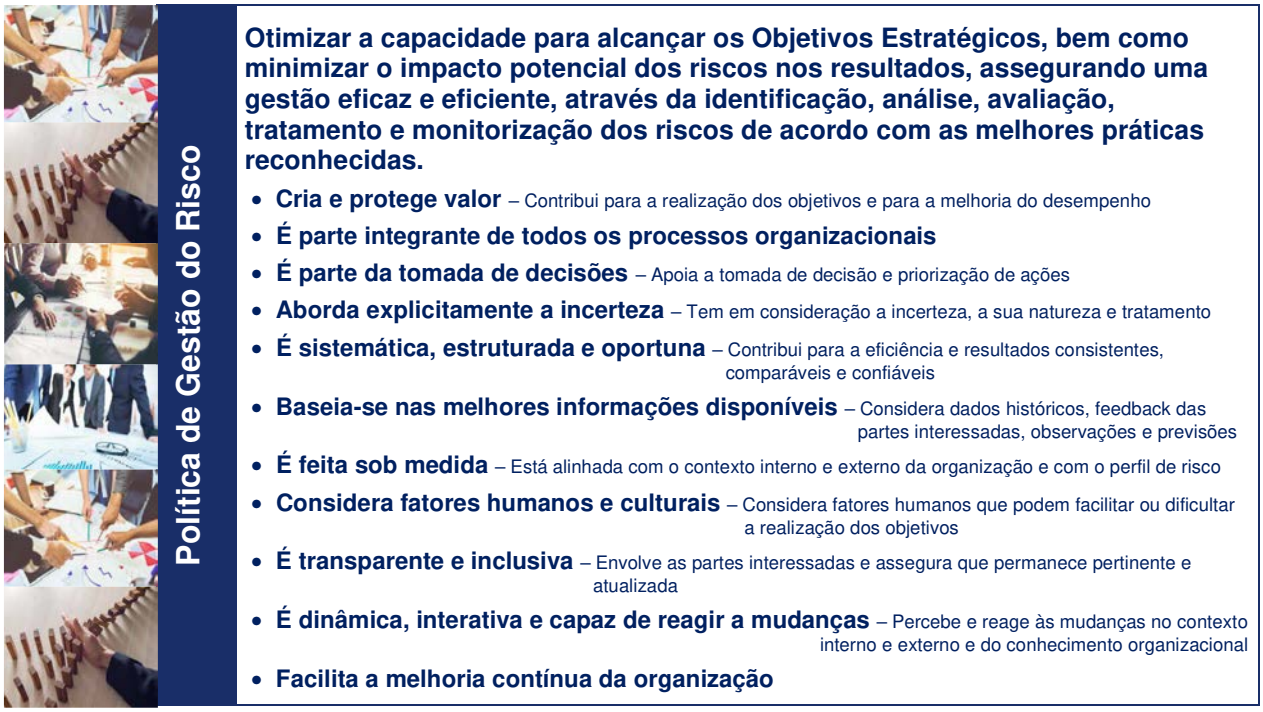
Quadro 5 – Prioridades Estratégicas do ISS, IP 2020

OE1	**Promover a coesão social e a inclusão**	
	PE 1.1	Reforçar o combate à pobreza e desigualdades
	PE 1.2	Promover a qualidade dos serviços e respostas sociais
	PE 1.3	Reforçar o acesso a serviços e equipamentos
OE2	**Garantir a sustentabilidade da Segurança Social**	
	PE 2.1	Aumentar a eficácia das prestações sociais reduzindo os prazos de deferimento e pagamento
	PE 2.2	Incrementar a eficiência das prestações sociais prevenindo a fraude e os pagamentos indevidos
	PE 2.3	Combater a fraude e a evasão garantindo o cumprimento das obrigações contributivas
OE3	**Reforçar a confiança na Segurança Social**	
	PE 3.1	Melhorar a qualidade e a capacidade de resposta ao cidadão
	PE 3.2	Assegurar o rigor e a qualidade dos procedimentos
	PE 3.3	Aumentar a satisfação das pessoas e das empresas
OE4	**Valorizar as pessoas e reforçar o orgulho organizacional**	
	PE 4.1	Desenvolver o potencial humano
	PE 4.2	Valorizar a cultura organizacional
	PE 4.3	Garantir um ambiente de trabalho feliz e saudável
OE5	**Modernizar e humanizar os serviços**	
	PE 5.1	Potenciar o acesso digital do cidadão aos serviços
	PE 5.2	Assegurar a eficiência da gestão dos recursos
	PE 5.3	Aumentar a sustentabilidade ambiental

3.1. Política de gestão de risco

A Política de Gestão do Risco do ISS, IP, foi aprovada em março de 2015.

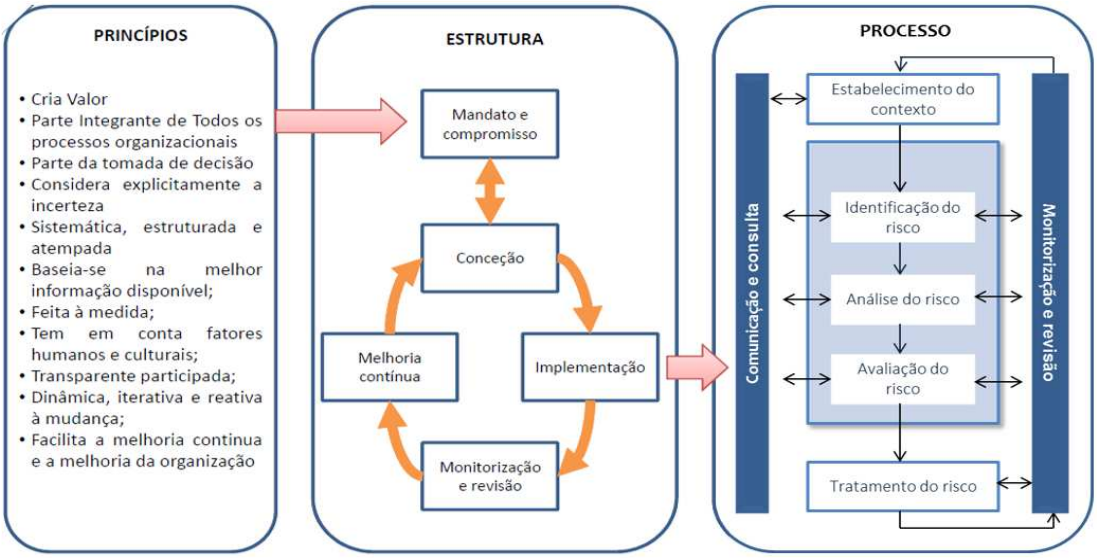
Figura 4 – Política da Gestão do Risco do ISS, IP



Conceptualmente, gerir riscos consiste no enfoque estruturado de alinhamento entre a estratégia, processos, pessoas, conhecimento organizacional e tecnologia, com objetivo de avaliar e controlar as incertezas inerentes com as quais as organizações se deparam, de forma a possibilitar a criação de valor.

Existem diversas abordagens para gerir riscos. Diferentes referenciais teóricos e modelos de trabalho sugerem contextos, que apesar de diferirem muitas vezes quanto às nomenclaturas utilizadas, convergem para os mesmos objetivos da atuação. Partindo desse pressuposto, a ISO 31000:2009 – Risk Management Principles and Guidelines – definiu uma abordagem integrada e assente no relacionamento entre os princípios para a gestão de risco, a estrutura na qual ocorre e o respetivo processo de gestão de risco. Esta abordagem esteve na base da definição do Modelo de Gestão de Risco em implementação no ISS, IP.

Figura 5 – Gestão do Risco



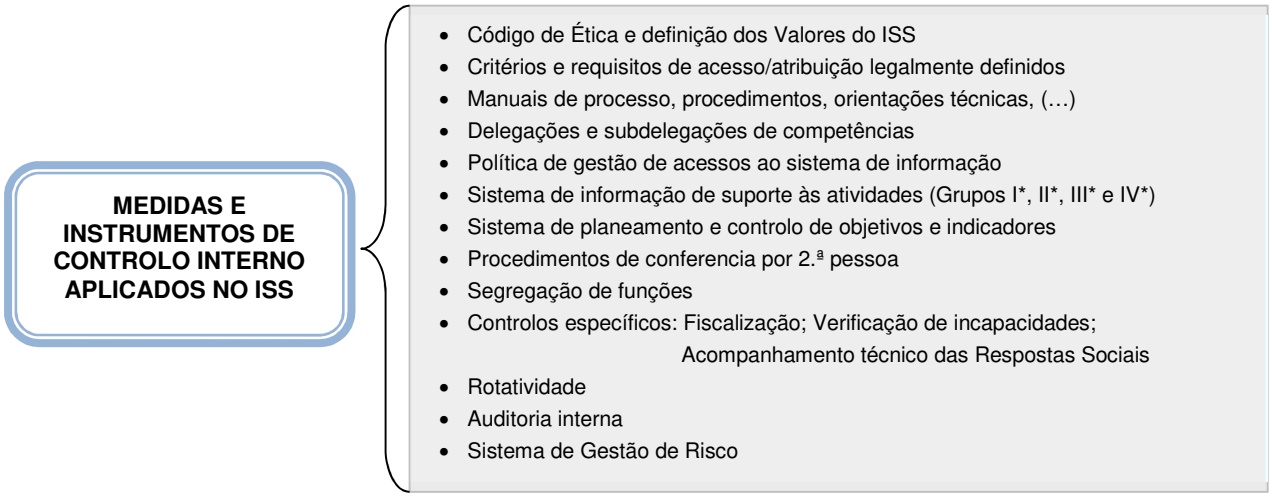
A incorporação da gestão do risco no ISS vem estabelecer um conjunto de práticas de identificação, análise, avaliação, tratamento, revisão, monitorização e reporte dos principais riscos.

As boas práticas de gestão de riscos contidas no guia da Ferma[1] identificam entre outros os seguintes princípios e orientações:

- A gestão de riscos aumenta as probabilidades de sucesso no alcance dos objetivos;
- A gestão de riscos deve ser integrada à cultura da organização, com uma política efetiva direcionada pela alta administração;
- A organização deve estabelecer critérios contra os quais os riscos são comparados;
- Os riscos devem ter proprietários;
- Separação clara de responsabilidades entre gestores, funções de apoio à governança e gestão dos riscos e auditoria interna.

O ISS, IP tem implementado mecanismos transversais, de natureza genérica, ao nível do sistema de controlo interno e gestão de risco. Trata-se de um conjunto de instrumentos de natureza variada, que cobrem todos os serviços do ISS, IP, de acordo com as funções desempenhadas, e que se complementam e articulam entre si, contribuindo, para a prevenção de diferentes eventos de risco.

Figura 6 – Medidas e Instrumentos de Controlo Interno Transversal



* Grupo I___Aplicações do âmbito de Prestações e Contribuições, bem como da Gestão e Controlo Financeiro: IDQ, GR, GC, GT, RPC, SEF e GTE;
* Grupo II___Aplicações do âmbito de Prestações e Contribuições, bem como da Gestão e Controlo Financeiro: DES, ITPT, CPA, PF, AF, CSI, RSI, SICC-PREST, SVI e FGS;
* Grupo III___Aplicações do âmbito do Desenvolvimento Social e Programas: ADOP, AS e COOP;
* Grupo IV Aplicações do âmbito da Fiscalização, Assuntos Jurídicos e Contencioso e Desenvolvimento Social e Programas: SAF, GIL, CO, CPF, PCAAC e CDF.

3.2. Estrutura de Gestão de Risco

A gestão de risco é suportada numa estrutura que se organiza e opera em consonância com a própria estrutura formal da organização, de forma a facilitar a fluidez e eficácia do processo.

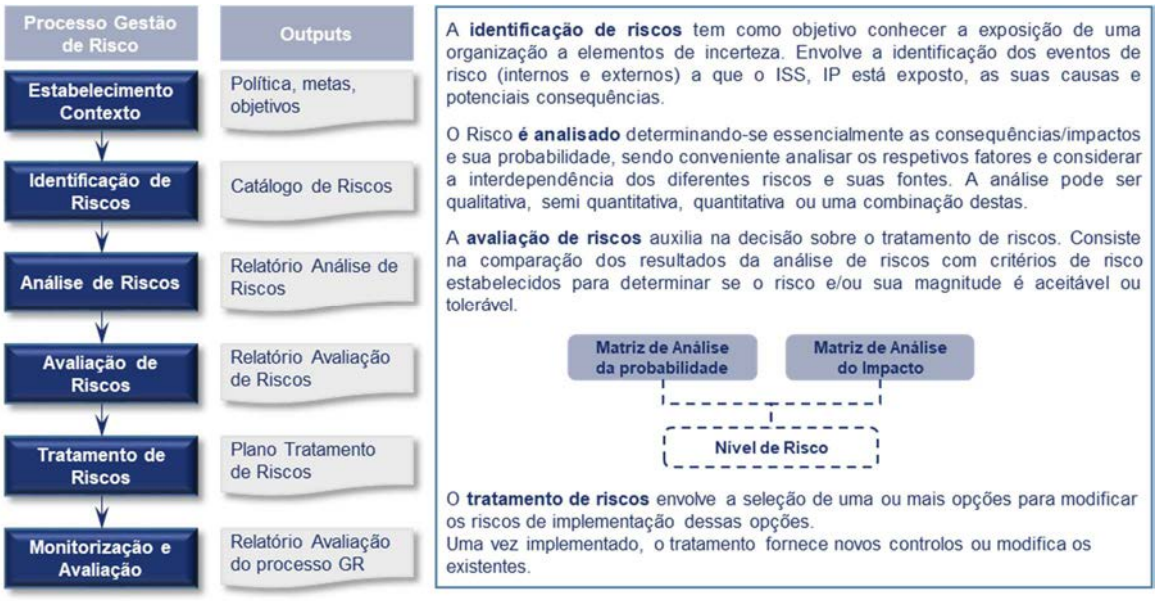
[1] O Risk Management Standard é um guia publicado pela Federation of European Risk Management Associations (Ferma) e resulta do esforço conjunto de diversas entidades europeias que atuam na promoção do uso da gestão de riscos pelas organizações em geral, inclusive do setor público (FERMA, 2003).

Figura 7 – Estrutura da Gestão de Risco

	Principais Intervenientes/stakeholders	Atribuições
Nível Estratégico	**Conselho Diretivo**	•Definir e aprovar a política de gestão de riscos; •Definir estratégia de gestão de risco; •Aprovar o Modelo de Gestão de Risco •Nomear e atribuir responsabilidades no âmbito da Gestão de Risco; •Assegurar os recursos necessários; •Aprovar riscos prioritários relevantes •Aprovar matriz de avaliação de riscos •Aprovar planos de tratamento do risco •Aprovar articulação com Stakeholders relevantes
Nível Tático	**Comissão de Gestão Risco** Permanentes: • Representante CD • GAQGR (Coord.) • GPE De acordo com âmbito: • Representante SC, CNP, CDist • Representante de Parte Interessada identificada • Técnicos da área G. Risco e/ou melhoria organizacional	•Propor melhorias ao Modelo de Gestão de Risco •Propor riscos prioritários •Propor gestores/equipas operacionais de gestão dos riscos •Validar matriz de avaliação de riscos •Analisar níveis de risco e prioriza riscos para tratamento •Validar Plano de Tratamento Global de Riscos •Validar os Relatórios Globais de Monitorização dos Riscos •Avaliar progresso Planos e níveis de risco •Identificar articulação com Stakeholders relevantes
	Equipa de Gestão de Risco GAQGR	•Definir e apoiar na implementação de um Modelo de Gestão de Risco •Propor à CGR riscos relevantes •Define Matriz de avaliação de riscos •Apoiar na identificação, análise e avaliação de riscos •Propor à CGR Plano Global de Tratamento de Riscos •Reportar o progresso do Plano Global de tratamento dos riscos •Assegurar a integração de informação dos diferentes gestores risco •Avaliar os resultados do desempenho da gestão de risco •Gestão dos riscos relevantes dos processos •Articular/consultar Stakeholders relevantes •Identificar, analisar e avaliar riscos
Nível Operacional	**Equipas operacionais** Unidades orgânicas Centrais Unidades orgânicas Desconcentradas	•Propor ações de melhoria •Definir planos de ação para tratamento do risco •Implementar e monitorizar o plano de ações necessárias •Reportar progresso EGR •Realimentar o do Modelo de Risco, alertando para novas situações de risco ou degradação do ambiente de controlo
	Auditoria	•Avaliar a implementação das medidas de tratamento dos riscos •Propor melhorias e alterações ao modelo de Gestão do Risco •Realimentar o Modelo de Gestão de Risco, alertando para novas situações de risco ou degradação do ambiente de controlo

4. Gestão de risco

Figura 8 - Processo Gestão de Riscos



4.1. Identificação de riscos

4.1.1. Catálogo de riscos

O catálogo de riscos identifica as principais tipologias de risco/eventos de incerteza a que o ISS se encontra exposto. Estes riscos foram definidos com base em referenciais metodológicos (FERMA, COSO) e atendendo à especificidade dos processos da organização.

Figura 9 – Catálogo de Riscos do ISS, IP

	RISCOS ESTRATÉGICOS	RISCOS FINANCEIROS	RISCOS OPERACIONAIS	RISCOS DISRUPTIVOS
CATEGORIAS DE RISCO	Riscos dependentes de contexto externo que podem afetar o cumprimento da missão.	Riscos associados ao desempenho financeiro e prestação de contas	Riscos associados ao desempenho dos processos, pessoas e recursos materiais, sistemas, ocorrendo de forma intencional ou não.	Risco com potencial para parar ou limitar seriamente as operações por períodos alargados de tempo, com severo impacto negativo.
CATEGORIAS DE RISCO (NÍVEL 1)	Riscos tecnológicos Riscos políticos Riscos económicos e sociais Riscos reputacionais	Riscos de contexto financeiro Riscos dos processos financeiros	Riscos de processos, projetos e programas Risco de recursos humanos e de pessoas. Riscos de saúde, segurança no trabalho e ambiente Riscos materiais e logísticos Riscos tecnológicos Riscos de conformidade legal/normativa Riscos de fraude interna Riscos de fraude externa Risco de violação de dados pessoais	Risco de recursos humanos ou risco de pessoas. Riscos tecnológicos Riscos materiais e logísticos Riscos naturais e ambientais Riscos de disrupção política, económica e social

4.2. Análise dos riscos

Com base no conjunto de riscos identificados, foi realizada uma avaliação da perceção dos dirigentes quanto à respetiva probabilidade de ocorrência e impactos na organização. Dos resultados do questionário, foi apurado um ranking de 5 categorias de risco prioritárias para o ISS, IP:

- Riscos estratégicos tecnológicos.
- Riscos operacionais:
  - Recursos humanos ou riscos de pessoas;
  - Riscos tecnológicos;
  - Fraude interna;
  - Fraude externa.

Com o objetivo complementar a avaliação da perceção existente no ISS, IP quanto aos riscos críticos e desenvolver uma análise quantitativa, capaz de fornecer uma compreensão sobre os mesmos e constituir um input importante para a definição de níveis de tolerância ao risco, foi desenvolvido um conjunto de atividades prévias:

- Mapeamento e compreensão dos riscos prioritários por relação às prioridades estratégicas.
- Análise dos riscos:
  - Identificação de eventos de risco: ocorrência ou alteração de um conjunto específico de circunstâncias;
  - Identificação de fatores: características ou circunstâncias que aumenta a probabilidade de ocorrência de um resultado desfavorável, de um dano ou de um fenômeno (in)desejado sem que intervenha necessariamente na sua causalidade.
- Construção de uma bateria de indicadores-chave de risco para estimar a sua incidência/ocorrência e impactos.
- Definição de critérios de integridade:
  - Adoção de indicadores de gestão já produzidos e disponíveis na organização;
  - Prevalência de indicadores recolhidos automaticamente.

A acrescer aos Riscos priorizados pela CGR, foi ainda incluída neste Plano o Risco de Violação de Dados Pessoais. Neste sentido foram identificados pelo EPD do ISS, IP 3 tipos de Violação de dados, descrevendo-os em eventos e com indicadores associados.

Numa análise global, foi relacionada a criticidade dos riscos à luz dos Objetivos Estratégicos do ISS, IP.

Quadro 6 – Mapeamento dos Risco / Prioridades Estratégicas

CATEGORIAS DE RISCO Nível 1	OBJETIVOS ESTRATÉGICOS				
	1 Promover a Coesão Social e a Inclusão	2 Garantir a Sustentabilidade da Segurança Social	3 Reforçar a Confiança Na Segurança Social	4 Valorizar as Pessoas	5 Modernizar e Humanizar os Serviços
Risco Operacional Recursos Humanos e Pessoas		✓	✓	✓	✓
Risco Operacional Tecnológico		✓	✓		
Risco Estratégico Tecnológico			✓		✓
Risco de Fraude Interna			✓		
Risco de Fraude Externa	✓	✓	✓		
Risco de Violação de Dados Pessoais			✓		

4.2.1. **Risco Operacional Recursos Humanos e Pessoas**

Como a organização gere, desenvolve e liberta o conhecimento e todo o potencial das pessoas que a compõem, quer ao nível individual, de equipa ou ao nível da organização no seu conjunto, e como planeia essas atividades de forma a prosseguir a política e a estratégia definidas e a garantir a eficácia operacional do seu pessoal, constitui um fator determinante na sua exposição a riscos.

Os riscos de insuficiência de recursos humanos, erros não intencionais e desajuste das qualificações e competências são percecionados pelos dirigentes do ISS, IP como riscos de grau elevado com impactos na prossecução da estratégia, desempenho dos processos e na imagem e reputação da organização.

Quadro 7 – Mapeamento dos Risco de Recursos Humanos e Pessoas por OE e PE

Risco nível 2	OE	Prioridade Estratégica
Risco de Quantidade	OE2	2.1. Aumentar a Eficácia das Prestações Sociais reduzindo os prazos de deferimento e pagamento
	OE3	3.1. Melhorar a qualidade e capacidade de resposta ao cidadão
Risco de Qualificação	OE3	3.1. Melhorar a qualidade e capacidade de resposta ao cidadão
		3.2. Assegurar o rigor e qualidade dos procedimentos
	OE4	4.1. Desenvolver o potencial humano
Risco de Clima Organizacional	OE4	4.3. Garantir um ambiente de trabalho feliz e saudável
Risco de Perda de Conhecimento	OE4	4.2. Valorizar a cultura organizacional
		4.3. Garantir um ambiente de trabalho feliz e saudável
	OE5	5.2 Assegurar a eficiência e gestão dos recursos

Para estimar o impacto destes riscos na estratégia da organização, procedeu-se à identificação de potenciais ocorrências de risco, fatores potenciadores dos mesmos e indicadores de incidência (probabilidade de ocorrência) e impacto.

Quadro 8 – Indicadores-chave de Risco Operacional de Recursos Humanos e Pessoas

CATEGORIA DE RISCO Nível 2	EVENTO	FATOR DE RISCO	INDICADOR
Risco de qualificação	Desajuste das competências/qualificações face às exigências das operações	Necessidades de formação	N.º de ações previstas em plano e não realizadas (por área)
			% de efetivos que não participou em ações de formação
		Capacidade produtiva	% de serviços com produtividades abaixo da produtividade do ISS, IP
Risco de erro não intencional	Erros na execução de operações por Indefinição de procedimentos	Indefinição de procedimentos	Ausência de manuais de processo
		Processos distorcidos	Não cumprimento dos procedimentos
		Erros nas decisões	Tx de recursos hierárquicos com provimento
Risco de quantidade	Insuficiência de RH para realização das operações	Necessidades RH	Tx de ocupação dos lugares QP
		Tempo de trabalho extra	N.º médio de horas acumuladas por trabalhador
			N.º médio de horas extraordinárias

CATEGORIA DE RISCO Nível 2	EVENTO	FATOR DE RISCO	INDICADOR
		Tempo de pendências	Prestações Sociais com tempo pendência superior a [definir] meses
Risco de clima organizacional	Conflito/mau relacionamento interpessoal	Saída por iniciativa do trabalhador	N.º de saídas de trabalhadores
		Comportamento disciplinar	N.º de processos disciplinares aos trabalhadores
		Colaboradores não satisfeitos/fraco envolvimento	Resultados dos inquéritos de satisfação aos trabalhadores
		Ausências/faltas do trabalhador	Tx de absentismo
Risco de perda de conhecimento	Perdas por saídas de colaboradores	Rotatividade/Turnover	N.º de saídas de trabalhadores vs n.º de entrada de trabalhadores por área

4.2.2. **Risco Operacional/Estratégico Tecnológico**

A era da transformação digital caracteriza-se essencialmente por uma mudança estrutural das organizações através da aplicação das tecnologias existentes e da incorporação de processos digitais que garantam a sua evolução para uma nova época.

A facilitação do acesso dos cidadãos aos serviços públicos e a simplificação e desmaterialização dos procedimentos administrativos continuam a ser identificados como formas de o Estado melhor servir os cidadãos, pelo que a modernização administrativa é apontada como um dos eixos estratégicos.

Quadro 9 – Mapeamento Risco Operacional/Estratégico Tecnológico

Risco nível 2	OE	Prioridade Estratégica
Risco de Falhas no Sistema	OE2	2.1. Aumentar a Eficácia das Prestações Sociais reduzindo ao prazos de deferimento e pagamento
		2.2 Incrementar a Eficiência das Prestações Sociais prevenindo a fraude e os pagamentos indevidos
		2.3 Combater a fraude e evasão garantindo o cumprimento das obrigações contributivas
	OE3	3.1. Melhorar a qualidade e capacidade de resposta ao cidadão
		3.3. Aumentar a satisfação das Pessoas e Empresas
Risco de Agilidade e Segurança da Informação	OE2	2.2 Incrementar a Eficiência das Prestações Sociais prevenindo a fraude e os pagamentos indevidos
		2.3 Combater a fraude e evasão garantindo o cumprimento das obrigações contributivas
	OE3	3.2. Assegurar o rigor e qualidade dos procedimentos
Risco de Software	OE3	3.1. Melhorar a qualidade e capacidade de resposta ao cidadão
	OE5	5.1 Potenciar o acesso digital aos serviços

Os riscos inerentes ao processo de modernização e transformação digital é real, no entanto, com procedimentos e gestão apropriada, é possível capitalizar as oportunidades, monitorizar e mitigar os riscos e endereçar os desafios que possam surgir nas mais distintas áreas - sistemas de TI, pessoas, processos e controlos. Para o efeito e no contexto das competências do ISS nesta matéria, foram selecionados fatores de risco e indicadores de monitorização.

Quadro 10 – Indicadores-chave de Risco Operacional/Estratégico Tecnológico

CATEGORIA DE RISCO Nível 2	EVENTO	FATOR DE RISCO	INDICADOR
RISCO OPERACIONAL TECNOLÓGICO			
Risco de falhas no sistema	Impossibilidade de continuidade dos processos decorrente de erros ou falhas nos sistemas de informação, (ex. interoperabilidade de dados, sistemas de processamento ou comunicação, …).	Falhas SI	Indisponibilidade dos sistemas informáticos
		Erros/desajustes SI	% de concretização de alterações aplicacionais
Riscos de agilidade e segurança da informação	Impossibilidade de receção, transmissão, armazenamento, processamento de informação em tempo útil e em segurança.	Acessos indevidos a informação	Análise dos perfis de acesso ao SISS
		Informação desatualizada	Tempo decorrido entre a receção da informação e o processamento
RISCO ESTRATÉGICO TECNOLÓGICO			
Risco de software	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.	Obsolescência/desajuste	% de pedidos de instalação de software não satisfeitos
			% de erros aplicacionais identificados em LGA e ainda não corrigidos

4.2.3. **Risco Operacional de Fraude Interna**

Os riscos de fraude interna, estão associados a diferentes atos e comportamentos praticados pelos agentes da organização. Trata-se de uma conduta ilegítima com vista a tirar vantagem para o próprio ou terceiros, ou a prejudicar a organização. Este risco pode imputar elevadas perdas numa organização, afetando igualmente a sua imagem e credibilidade.

Os eventos de fraude interna podem tipificar-se em três grandes categorias de riscos (criminalmente individualizados, com requisitos específicos legalmente previstos), nomeadamente: apropriação indevida, corrupção e informações fraudulentas.

A fraude interna é percecionada no ISS como um risco com impactos muito elevados na imagem e reputação da organização.

Quadro 11 – Mapeamento Risco Operacional Fraude Interna

Risco nível 2	OE	Prioridade Estratégica
Corrupção e Infrações Conexas	OE3	3.2. Assegurar o Rigor e a Qualidade dos Procedimentos
Apropriação Indevida		
Outras ações Fraudulentas		

Quadro 12 – Indicadores-chave de Risco Operacional Fraude Interna

CATEGORIA DE RISCO Nível 2	EVENTO	FATOR DE RISCO	INDICADOR
Corrupção e Infrações Conexas	Atos ou sua omissão seja, lícito ou ilícito, por parte de colaborador da organização, com vista ao recebimento ou a promessa de uma qualquer compensação que não seja devida, para o próprio ou para terceiro: abuso de poder; peculato; participação económica em negócio; concussão; tráfico de influências; suborno.	Inexistência/falhas nos mecanismos de controlo interno	Não conformidades apuradas em sede de auditoria
Apropriação Indevida	Apropriação ilegítima ou por permissão intencional de apropriação ilegítima por outrem, por quem, por força do cargo que desempenha, (administração, gerência, outra…) tenha a capacidade de dispor de bens do setor publico ou cooperativo.	Inexistência/falhas nos mecanismos de controlo interno	Não conformidades apuradas em processos de auditoria
Outras Ações Fraudulentas	Burla; Conluio e/ou Cumplicidade; Erro intencional; Falsas declarações; Falsificação de dados e/ou documentos; Omissão intencional; Violação de deveres profissionais; Violação de outros deveres inerentes à função (dever de isenção); Violação de outros deveres inerentes à função (dever de zelo); Violação de segredo profissional	Inexistência/falhas nos mecanismos de controlo interno	Não conformidades apuradas em processos de auditoria

4.2.4. **Risco Operacional de Fraude Externa**

A arrecadação de receitas da Segurança Social constitui-se como alicerce fundamental para aumentar os recursos financeiros do sistema e aprofundar a sua sustentabilidade. A arrecadação de receitas que não resultem do pagamento atempado de obrigações contributivas, ou da devolução voluntária de prestações indevidas, assenta necessariamente na recuperação das perdas associadas à evasão contributiva e fraude prestacional, cujo sucesso tem, para além dos resultados financeiros, um reflexo direto no aumento da confiança dos cidadãos no sistema.

Quadro 13 – Mapeamento Risco Operacional Fraude Externa

Risco nível 2	OE	Prioridade Estratégica
Evasão a Obrigação Contributiva	OE2	2.2 Incrementar a Eficiência das Prestações Sociais prevenindo a fraude e os pagamentos indevidos
		2.3 Combater a fraude e evasão garantindo o cumprimento das obrigações contributivas
	OE3	3.2. Assegurar o Rigor e a Qualidade de Procedimentos
Acesso Indevido a Direito	OE1	1.2. Promover a Qualidade dos Serviços e Respostas Sociais
	OE2	2.2 Incrementar a Eficiência das Prestações Sociais prevenindo a fraude e os pagamentos indevidos
		2.3 Combater a fraude e evasão garantindo o cumprimento das obrigações contributivas

A fraude externa consiste essencialmente em perdas associadas a evasão contributiva e acesso indevido a direitos decorrentes de manipulação de informação, falsificação de documentos, falsas declarações, omissão de informação e aproveitamento de fragilidades. Medir a ocorrência e impacto destes riscos, exige a seleção de indicadores que orientem a definição de níveis de tolerância e ações de mitigação.

Quadro 14 – Indicadores-chave de Risco Operacional Fraude Externa

CATEGORIA DE RISCO Nível 2	EVENTO	FATOR DE RISCO	INDICADOR
Evasão a obrigações contributivas	Perdas por manipulação de informação; falsificação de documentos; falsas declarações; omissão de informação; aproveitamento de fragilidades.	Inexistência/falhas nos mecanismos de controlo (irregularidades/dívida contributiva)	% de dívida participada
			N.º de DR anuladas
			Contribuições apuradas e anuladas
	Contribuições não declaradas; Não entrega das quotizações retidas aos trabalhadores	Inexistência/falhas nos mecanismos de controlo (abuso de confiança)	Montante das contribuições apuradas
			Processos de Inquérito Crime (Abuso de confiança)
		Inexistência/falhas nos mecanismos de controlo (irregularidades/ contraordenações)	Montante de coimas notificado de CO (M€)
			Montante arrecadado de pagamentos voluntários de CO (M€)
			% de participações de infrações para CO
			% Processos CO do ano decididos

CATEGORIA DE RISCO Nível 2	EVENTO	FATOR DE RISCO	INDICADOR
Acesso indevido a direitos	Manipulação de informação; falsificação de documentos; falsas declarações; omissão de informação; aproveitamento de fragilidades.	Inexistência/desajuste de acompanhamento	% de processos de fiscalização a equipamentos sociais com irregularidades
			Controle de frequências nas respostas sociais
			% de ações de acompanhamento na sequência de processos de fiscalização
		Inexistência/falhas nos mecanismos de controlo	% de não conformidades detetadas no âmbito das Medidas de Apoio Excecional
			Notas de reposição emitidas (por apoio)
	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	Inexistência/falhas nos mecanismos de controlo (Burla)	Análise de DR retroativas
			Montante das contribuições falsas – constante de DR forjadas
			Processos de Inquérito Crime (Burla)
			% de pagamentos indevidos face ao total de prestações/apoios pagas(os) (por prestação/apoio)
			N.º de processos inquérito crime
			Acompanhamento da execução financeira de programas e apoios extraordinários

4.2.5. **Risco Operacional de Violação de Dados Pessoais**

A violação de dados pessoais consiste na "[…] violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados, ada dos pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" [2]

Na sua aceção mais genérica e de acordo com o Parecer 03/2014 da Comissão Nacional de Proteção de Dados (CNPD), relativo à notificação de violação, podem existir 3 Tipos de violações de dados pessoais categorizadas com os três princípios de segurança da informação:

- Violação da confidencialidade - quando existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais.
- Violação da integridade - quando existe uma alteração acidental ou não autorizada dos dados pessoais.
- Violação da disponibilidade - quando existe uma perda de acesso ou a destruição acidental ou não autorizada de dados pessoais.

Quadro 15 – Mapeamento Risco Operacional de violação de dados pessoais

Risco nível 2	OE	Prioridade Estratégica
Violação da confidencialidade	OE3	3.2. Assegurar o Rigor e a Qualidade de Procedimentos
Violação da integridade		
Violação da disponibilidade		

[2] Definição do art.º 4º, n.º 12 do RGPD.

Quadro 16 – Indicadores-chave de Risco Operacional de Violação de Dados Pessoais

CATEGORIA DE RISCO Nível 2	EVENTO	FATOR DE RISCO	INDICADOR
Violação da confidencialidade	Perdas decorrentes de situação em que existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais.	Insuficiência/desajuste dos mecanismos de controlo	Total de incidentes de violação recebidos
			% de Incidentes respondidos com apuramento dos factos
Violação da integridade	Perdas por alteração acidental ou não autorizada dos dados pessoais.	Insuficiência/desajuste dos mecanismos de controlo	Total de incidentes de violação recebidos
			% de Incidentes respondidos com apuramento dos factos
Violação da disponibilidade	Perdas de acesso ou a destruição acidental ou não autorizada de dados pessoais.	Insuficiência/desajuste dos mecanismos de controlo	Taxa de Incidentes de Segurança Informação
			Tempo Médio Resolução de Incidentes de Segurança
			Tempo médio reposição da disponibilidade dos serviços online
			Disponibilidade média dos serviços
			Nº de incidentes de indisponibilidade

5. Evolução do Plano

Do presente Plano resulta um conjunto de informação intermédia de suporte à estimativa da incidência e impactos dos riscos no desempenho da organização.

Decorrente da sua aprovação, serão acauteladas as condições de recolha e produção dos indicadores-chave selecionados junto das áreas intervenientes, para um histórico dos últimos anos (2015-1019).

A estimativa da probabilidade/impacto para este período, constituirá a base para a definição de critérios de tolerância, a partir dos quais serão determinados os parâmetros da matriz de avaliação (Figura 10 - Matriz de Risco).

Figura 10 – Matriz de avaliação de Risco

Impacto			
Nível de Risco	**Financeiro**	**Reputacional**	**Operacional**
	Perdas diretas e indiretas sobre valores e bens	Perdas de credibilidade da organização Violação dos princípios de interesse público	Falha no cumprimento dos objetivos
1- Baixo	Sem potencial prejuízo financeiro	Sem prejuízo da imagem	Sem impacto no cumprimento dos objetivos estratégicos. Nenhum requisito de Negócio afetado
2- Médio	Pode provocar prejuízo financeiro	Com prejuízo de imagem	Com impacto moderado no cumprimento dos objetivos estratégicos. Alguns requisitos de negócio em incumprimento
3- Alto	Pode provocar grave prejuízo financeiro	Grave prejuízo da imagem Violação grave dos princípios de interesse público	Com impacto elevado no cumprimento de 1 ou mais objetivos estratégicos. Objetivo estratégicos em incumprimento

Probabilidade de ocorrência	
1- Baixa	Atividade pontual, em situações excecionais
2- Média	Atividade que pode ocorrer no ano
3- Alta	Atividade corrente e frequente no Instituto

Nível de risco		Impacto		
		Baixo (1)	Médio (2)	Alto (3)
Probabilidade	Baixo (1)	**1**	**2**	**3**
	Médio (2)	**2**	**4**	**6**
	Alto (3)	**3**	**6**	**9**

O nível de risco apurado pela aplicação dos critérios de avaliação, determina o tipo de ação a desenvolver.

Nível de Risco	Ação
Baixo	Monitorizar Risco
Médio	Manter avaliação da efetividade dos controlos de risco existentes
Alto	Elaborar plano de ação para introdução de controlos mais eficazes

Na fase seguinte, de avaliação dos riscos, são comparados os resultados apurados na análise com os níveis de tolerância de risco estabelecidos para a organização, determinando-se o nível de risco e a ação a implementar pela aplicação da matriz de avaliação.

Figura 11 – Próximos Passos