AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA

Guia de Operacionalização: Segurança de Informação

ÍNDICE

ÍNDICE

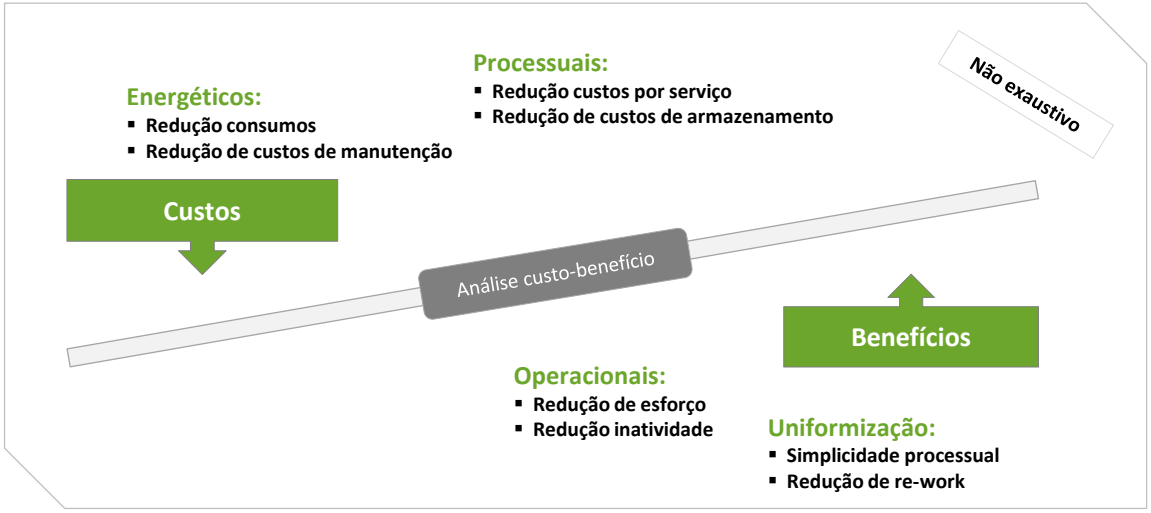
1. Introdução

1.1 Enquadramento

A **Agência para a Modernização Administrativa, I.P. (AMA)** tem por missão identificar, desenvolver e avaliar programas, projetos e ações de modernização e de simplificação administrativa e regulatória e promover, coordenar, gerir e avaliar o sistema de distribuição de serviços públicos, no quadro das políticas definidas pelo Governo.

Englobado na **Medida 4 do Plano Global Estratégico de Racionalização e Redução de Custos nas TIC** (Tecnologias de Informação e Comunicações) na Administração Pública (PGETIC), propõe-se **a criação de um modelo transversal aplicável a todos os ministérios** de forma a **medir e avaliar os resultados da implementação das medidas de racionalização**.

Neste sentido, propõe-se **a criação de um modelo transversal bem como uma ferramenta de suporte ao modelo** de forma a **apoiar o apuramento de benefícios e redução de custos.**



ÍNDICE

1. Introdução

1.2 Objetivos

O presente documento surge como **Guia de Suporte à operacionalização do modelo de avaliação de medidas no âmbito da Segurança de informação**, tendo os seguintes objetivos específicos:

1. **Apresentação da metodologia genérica para o apuramento de benefícios e redução de custos**, incluindo a diferenciação entre componentes TIC e não TIC, assim como a ferramenta de suporte à sua operacionalização.

2. **Descrição das variáveis e indicadores que compõem o modelo de apuramento de benefícios e redução de custos**, detalhando o modelo de cálculo das variáveis.

Notas:

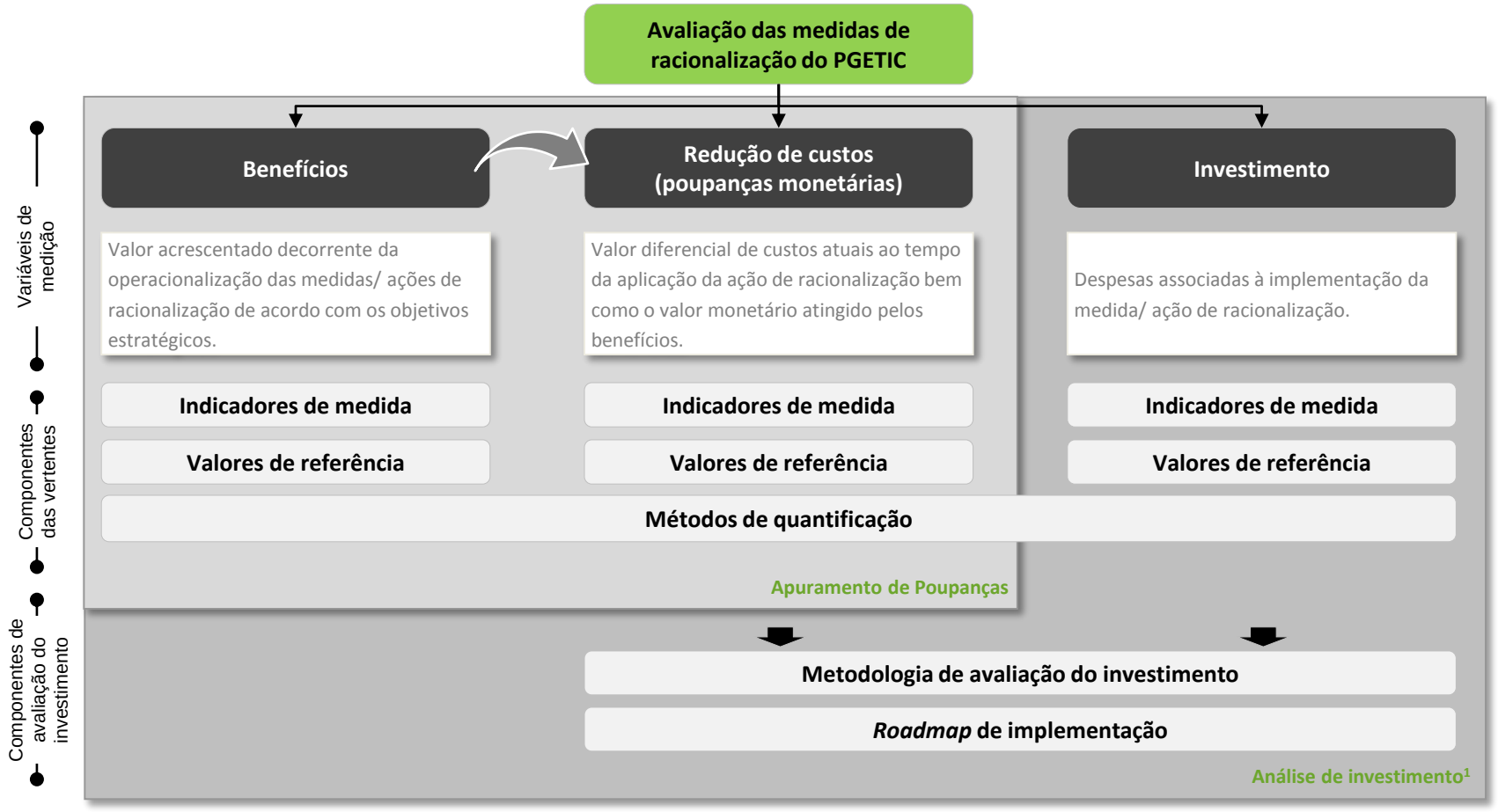
1. No sentido de apoiar a utilização da ferramenta de suporte, deve ser consultar o documento Manual de Utilizador.
2. No caso específico do modelo de segurança de informação, não se considera a redução de custos direta derivado da sua operacionalização.

ÍNDICE

1. Introdução

1.3 Metodologia (1/3)

A concretização da análise custo-benefício por cada tipologia de ação será determinada pelo **apuramento de benefícios, redução de custos e respetivo investimento associado às ações de racionalização**:



[1] Os modelos de ACB recomendam um período de análise de 4 anos como o domínio temporal ideal para serem refletidos resultados fidedignos.
Fonte: HM Treasury – cost benefit analysis guidance

1. Introdução

1.3 Metodologia (2/3)

A correta utilização da ferramenta de apoio e a operacionalização do apuramento de benefícios e redução de custos **prossupõe o entendimento dos seguintes conceitos base**:

Indicadores de medição

- Valores monitorizados **de acordo com a progressão da implementação da ação.**
- **Necessário preenchimento por parte do utilizador**, de modo frequente e adaptado á realidade ministerial em causa.
- Tipicamente serão **recolhidos valores relativos a domínios temporais antes e após da implementação** da ação a medir.

Valores de referência

- **Dados previamente recolhidos da literatura** assumindo as **melhores práticas internacionais** nas respetivas áreas de atuação.
- A maioria destes valores de referência **já estão pré-preenchidos na ferramenta** sendo **possível, sempre que necessário, o seu ajuste á realidade**.

Variáveis de medição

- Parâmetros de **calculo automático através da conjugação de indicadores de medição e valores de referência**.
- **Existem campos de preenchimento adicionais** na eventualidade de o utilizador necessitar de **acrescentar variáveis não identificadas na ferramenta**.

Exemplos

Virtualização de servidores

Valor à data de referência Nº de servidores físicos sem virtualização	100
Valor à data atual Nº de servidores físicos sem virtualização	7
Consumo energético por servidor	40 Kwh
Redução de custos: Poupanças energéticas =	$[100 - 7]\ x\ 40$

Apuramento dos benefícios e redução de custos TIC/ Não TIC pelo agrupamento das diversas variáveis de medição calculadas

Nota: Os valores monetários são referentes a montantes sem IVA.

1. Introdução

1.3 Metodologia (3/3)

Por forma a **otimizar e sistematizar o apuramento de benefícios e redução de custos** foi desenvolvida uma ferramenta de suporte de utilização transversal a todos os ministérios que se caracteriza por:

Premissas:

Simplicidade + **Robustez**

Eficiência

Garantir que a complexidade associada ao apuramento permite uma **aplicação ágil do modelo**.

Clareza

Assegurar que o modelo seja **inteligível e de fácil compreensão**.

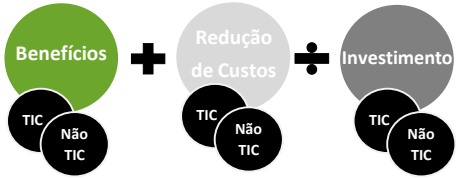
Coerência

Sustentar a **conformidade entre análises e a coerência** de metodologias.

Detalhe

Conferir elevado **grau de exaustividade** face aos objetivos definidos.

Abordagem:



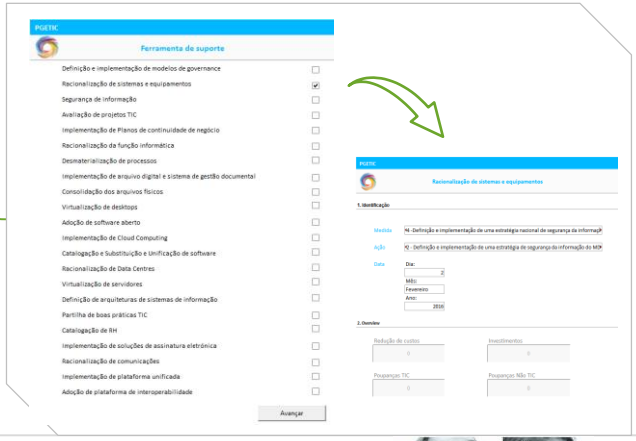
As poupanças alcançadas serão mensuradas pelo cálculo do retorno de investimento financeiro que se traduz pela divisão da soma dos custos e benefícios pelo valor monetário investido na implementação.

Apuramento de Benefícios e Redução de Custos

Tecnologia utilizada:

O **LibreOffice é uma Open Source** que inclui folhas de cálculo úteis no cálculo, análise e gestão de dados. Esta ferramenta possui o formato ODF como padrão, permitindo a exportação de arquivos em PDF sem a necessidade de instalação de extensões.

Ilustrativos:



ÍNDICE

2. Modelo de avaliação

2.1 Enquadramento da tipologia de ação

A segurança da informação está diretamente relacionada **com a proteção de conjuntos de informações e visa a preservação do valor organizacional que estas possuem**:

O conceito de segurança de informação **não se restringe apenas a sistemas computacionais, abrangendo igualmente temas como transferência de dados digitais e cumprimento do quadro legal de segurança**. Neste sentido, o modelo de análise custo-benefício definido incide em 3 vertentes.

		Exemplos de ações setoriais englobadas:
Cibersegurança	▪ Refere-se ao conjunto de meios e tecnologias que visam proteger de danos e intrusão ilícita. ▪ Engloba barreiras lógicas que impedem ou limitam o acesso a informação, como por exemplo firewalls e anti-vírus.	Criação, instalação e operacionalização do Centro Nacional de Cibersegurança.
Integridade de dados	▪ Abrange a não exposição da informação, evitando o manuseio/ alteração não autorizado. ▪ Caracteriza-se por procedimentos de transformação reversível da informação de forma a torná-la ininteligível a terceiros bem como de validações de certificações corporativas.	Expansão da solução de criptografia nacional.
Procedimentos e Normas	▪ Traduz o cumprimento do quadro legal de segurança pela consciencialização governamental de boas práticas e princípios fundamentais. ▪ Especifica comportamentos atempados de cooperação de forma a prevenir, detetar e reagir a incidentes de segurança.	Definição de normas e *guidelines* de Segurança.

ÍNDICE

2. Modelo de avaliação

2.2 Indicadores de medição (1/3)

Indicadores de medição para apuramento de benefícios

	Indicador de medição	*Descrição*	*Unidade*	*Obrigatoriedade*
1	**Número médio de registos informáticos comprometidos (Valor de referência)**	Número de registos/ dados informáticos comprometidos devido a quebras de segurança, quer por ações internas (e.g. fraude interna) quer por ações externas (e.g. ataques informáticos), tendo como referência o ano de 2011.	Numérico	Preenchimento obrigatório
2	**Número de registos informáticos comprometidos (Valor à data atual)**	Número de registos/ dados informáticos comprometidos devido a quebras de segurança, quer por ações internas (e.g. fraude interna) quer por ações externas (e.g. ataques informáticos) à data atual.	Numérico	Preenchimento obrigatório
3	**Número de *endpoints* (Valor à data atual)**	Volume de *endpoints* ativos, i.e. terminais tecnológicos utilizados pelos colaboradores (e.g. computadores, telemóveis, entre outros)à data atual.	Numérico	Preenchimento obrigatório
4	**Número de *endpoints* extraviados com informação sensível/ confidencial com encriptação (Valor à data atual)**	Número de *endpoints* extraviados com informação sensível e/ ou confidencial, com sistemas de encriptação já incorporados à data atual.	Numérico	Preenchimento obrigatório
5	**Número de incidentes derivado de infeções informáticas (e.g. vírus) (Valor de referência)**	Número de incidentes informáticos registados com origem em infeções informáticas, tendo como alvo os sistemas de informação do Ministério, tendo como referência o ano de 2011.	Numérico	Preenchimento obrigatório
6	**Número de incidentes derivado de infeções informáticas (e.g. vírus) (Valor à data atual)**	Número de incidentes informáticos registados com origem em infeções informáticas, tendo como alvo os sistemas de informação do Ministério à data atual.	Numérico	Preenchimento obrigatório
7	**Número total de infeções informáticas**	Número total de infeções informáticas ocorridas durante o período em análise.	Numérico	Preenchimento obrigatório

2. Modelo de avaliação

2.2 Indicadores de medição (2/3)

Indicadores de medição para apuramento de benefícios

	Indicador de medição	*Descrição*	*Unidade*	*Obrigatoriedade*
8	**Existência de Chief Information Security Officer?**	Aferição da existência de um *Chief Information Security Officer* no Ministério, devendo ser escolhidas as opções “Sim” ou “Não”.	Binário	Preenchimento obrigatório
9	**Existência de PCN implementado?**	Aferição da existência de um Plano de Continuidade de Negócio implementado e ativo no Ministério, devendo ser escolhidas as opções “Sim” ou “Não”.	Binário	Preenchimento obrigatório
10	**Existência de plano de resposta a incidentes informáticos?**	Aferição da existência de um Plano de Resposta a Incidentes Informáticos no Ministério, devendo ser escolhidas as opções “Sim” ou “Não”.	Binário	Preenchimento obrigatório

2. Modelo de avaliação

2.2 Indicadores de medição (3/3)

Indicadores de medição para apuramento de investimentos

	Indicador de medição	*Descrição*	*Unidade*	*Obrigatoriedade*
11	**Custos de formação**	Custo de formação dos recursos humanos necessária para a implementação da iniciativa de Sistemas de informação.	€	Facultativo caso tenha ocorrido investimento
12	**Custos de integração de sistemas**	Custo de integração de sistemas necessária para a implementação da iniciativa de Sistemas de informação.	€	Facultativo caso tenha ocorrido investimento
13	**Custos de licenciamento de SW**	Custo de licenciamento de software necessário para a implementação da iniciativa de Sistemas de informação.	€	Facultativo caso tenha ocorrido investimento
14	**Custos de migração**	Custo de migração de sistemas para a implementação da iniciativa de Sistemas de informação.	€	Facultativo caso tenha ocorrido investimento
15	**Custos de setup**	Custo de setup para a implementação da iniciativa de Sistemas de informação.	€	Facultativo caso tenha ocorrido investimento
16	**Custos aquisição de serviços de consultoria/ estudos**	Custo de aquisição e serviços externos de consultoria, estudo ou apoio à implementação da iniciativa Sistemas de informação.	€	Facultativo caso tenha ocorrido investimento
17	**Custos de infraestrutura de comunicações**	Custo de infraestrutura de comunicações necessária para a implementação da iniciativa de Sistemas de informação.	€	Facultativo caso tenha ocorrido investimento
18	**Custos de aquisições de HW**	Custo de hardware necessário para a implementação da iniciativa de Sistemas de informação.	€	Facultativo caso tenha ocorrido investimento

ÍNDICE

2. Modelo de avaliação

2.3 Valores de referência

Valores de referência para apuramento de reduções de custos

	Valor de referência	*Descrição*	*Referência*	*Unidade*
19	Taxa de vírus evitados em sistemas considerados seguros	Percentagem de vírus evitados acima da qual um sistema é considerado seguro, correspondendo a 84%.	Intel – The Cost of a Lost Laptop	%
20	Taxa de *endpoints* corrompidos em sistemas seguros	Percentagem de *endpoints* corrompidos abaixo da qual um sistema é considerado seguro, correspondendo a 11%.	IBM – Cost of Data Breach	%
21	Poupança associada ao extravio de um *endpoint* encriptado vs. Não encriptado com informação sensível/ confidencial no setor Governamental	Valor monetário relativo ao gasto evitado no extravio de um *endpoint* caso este esteja encriptado (comparativamente ao extravio de *endpoint* não encriptado), correspondendo a 3.041€ por *endpoint*.	Intel – The Cost of a Lost Laptop	€
22	Custo de incidente causado por infeções informáticas	Custo para a organização associado a um incidente informático oriundo de infeções informáticas, correspondendo a 24711€.	Intel – The Cost of a Lost Laptop	€
23	Custo associado a um registo informático comprometido em ataque informático	Custo para a organização relativo a um registo informático comprometido devido a um ataque informático, correspondendo a 118€/ registo.	ICSA - Labs Virus Prevalence Survey 1904	€
24	Diminuição do custo associado a um registo informático comprometido em ataque informático com cargo de CISO nomeado	Diminuição do custo associado a um registo informático comprometido em ataque informático caso esteja implementado um *Chief Information Security Officer*, correspondendo a 5,88€.	ICSA - Labs Virus Prevalence Survey 1904	€
25	Diminuição do custo associado a um registo informático comprometido em ataque informático com PCN implementado	Diminuição do custo associado a um registo informático comprometido em ataque informático caso esteja implementado um Plano de Continuidade de Negócio implementado, correspondendo a 6€.	ICSA - Labs Virus Prevalence Survey 1904	€
26	Diminuição do custo associado a um registo informático comprometido em ataque informático com plano de resposta a incidentes definido	Diminuição do custo associado a um registo informático comprometido em ataque informático caso esteja implementado um plano de resposta a incidentes definido, correspondendo a 11,39€.	ICSA - Labs Virus Prevalence Survey 1904	€

Nota: Os valores apresentados incluem o IVA à taxa legal em vigor

ÍNDICE

2. Modelo de avaliação

2.4 Variáveis de medição (1/3)

Variáveis de medição

B9 – Continuidade de negócio e recuperação de incidentes

B9.1 **Redução do número de registos comprometidos (#):** aferição da evolução do número de registos/ dados informáticos comprometidos, após a implementação de medidas de segurança de informação.

Fórmula de cálculo

(1) - (2)

B9.2 **Redução do número de incidentes derivados de infeções informáticas (#):** evolução do número de incidentes com origem em infeções informáticas, após a implementação de medidas de segurança de informação.

Fórmula de cálculo

(5) - (6)

Indicadores de mediação e valores de referência utilizados

1. Número médio de registos informáticos comprometidos (Valor de referência)
2. Número médio de registos informáticos comprometidos (Valor à data atual)
5. Número de incidentes derivado de infeções informáticas (e.g. virus) (Valor de referência)
6. Número de incidentes derivado de infeções informáticas (e.g. virus) (Valor à data atual)

2. Modelo de avaliação

2.4 Variáveis de medição (2/3)

Variáveis de medição

B9 – Continuidade de negócio e recuperação de incidentes

B9.5 **Custos evitados com extravio de *endpoints* (€):** custos evitados associados a extravio de *endpoints* com informação sensível/ confidencial com encriptação.

Fórmula de cálculo

4 * 20 * 21

B9.6 **Cobertura de *endpoints* com encriptação (%):** aferição do grau de *endpoints* com implementação de sistemas de encriptação.

Fórmula de cálculo

4 / 3

Indicadores de mediação e valores de referência utilizados

3	Número de *endpoints* (Valor à data atual)	20	Taxa de *endpoints* corrompidos em sistemas seguros
4	Número de endpoints extraviados com informação sensível e/ ou confidencial, com sistemas de encriptação já incorporados à data atual.	21	Poupança associada ao extravio de um endpoint encriptado vs. Não encriptado com informação sensível/ confidencial no setor Governamental

Benefícios utilizados

B9.2	Número de incidentes derivados de infeções informáticas
B8.7	Variação da cobertura de *endpoints* com encriptação

2. Modelo de avaliação

2.4 Variáveis de medição (3/3)

Variáveis de medição

B9 – Continuidade de negócio e recuperação de incidentes

B9.3 **Custos evitados com registos informáticos comprometidos (€):** custos evitados associados a registos informáticos comprometidos, face à situação de referência.

Fórmula de cálculo

B9.1 *(23 - 8 *24 - 9 *25 - 10 *26)

B9.4 **Custos evitados com infeções informáticas (€):** custos evitados associados a infeções informáticas bem sucedidas, face ao mínimo admissível para ser considerado um sistema seguro.

Fórmula de cálculo

(6 - 7 *19)* 22

Indicadores de mediação e valores de referência utilizados

6	Número de incidentes derivado de infeções informáticas (e.g. vírus) (Valor à data atual)
7	Número total de infeções informáticas
8	Existência de *Chief Information Security Officer*?
9	Existência de PCN implementado?
10	Existência de plano de resposta a incidentes informáticos?
19	Taxa de vírus evitados em sistemas considerados seguros
22	Custo de incidente causado por infeções informáticas
23	Custo para a organização relativo a um registo informático comprometido devido a um ataque informático, correspondendo a 118€/ registo.
24	Diminuição do custo associado a um registo informático comprometido em ataque informático com cargo de CISO nomeado
25	Diminuição do custo associado a um registo informático comprometido em ataque informático com PCN implementado
26	Diminuição do custo associado a um registo informático comprometido em ataque informático com plano de resposta a incidentes definido

Benefícios utilizados

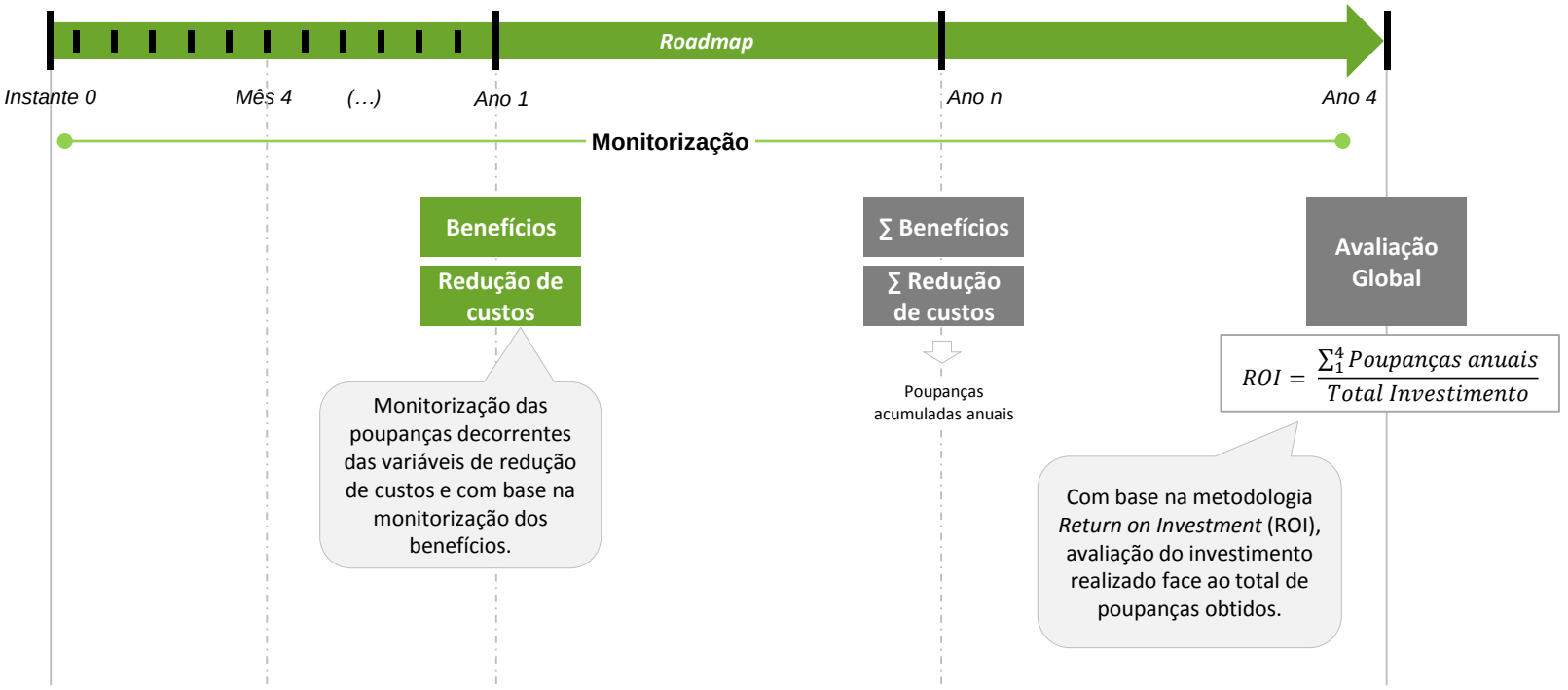
B9.1	Redução do número de registos comprometidos

ÍNDICE

2. Modelo de avaliação

2.5 *Roadmap* de monitorização e avaliação

Dada a natureza desta tipologia de ação, recomenda-se a aplicação do modelo numa **base anual** na qual devem ser revistas as **variáveis de medição**.



Nota: Os modelos de ACB recomendam um período de análise de 4 anos como o domínio temporal ideal para serem refletidos resultados fidedignos.
Fonte: HM Treasury – cost benefit analysis guidance

AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA