Universidade Católica Portuguesa

Faculdade de Engenharia

Gestão do Conhecimento – Modelação dos Incidentes e das Respostas

Francisco Manuel de Sousa Canelas Lopes

Dissertação para obtenção de Grau de Mestre em Segurança em Sistemas de Informação

Júri

Prof. Doutor Rui Jorge Correia Mendes Alves Pires (Presidente)

Profª. Doutora Helena Sofia Andrade Nunes Pereira Pinto

Prof. Doutor Tito Lívio dos Santos Silva (Orientador)

Novembro de 2010

Universidade Católica Portuguesa

Faculdade de Engenharia

Gestão do Conhecimento – Modelação dos Incidentes e das Respostas

Francisco Manuel de Sousa Canelas Lopes

Dissertação para obtenção de Grau de Mestre em Segurança em Sistemas de Informação

Orientador: Prof. Tito Santos Silva

Co-orientador: Eng. Maria Raquel César

Novembro de 2010

Resumo

Este trabalho pretende demonstrar que as políticas de gestão de uma organização podem ter influência directa na segurança de informação, não bastando apenas o recurso à tecnologia para a sua eficaz protecção.

Neste sentido a Gestão do Conhecimento pode contribuir positivamente, tendo em conta o desenvolvimento e a autonomia dos indivíduos que integram e constituem a organização, estimulando a partilha da informação, a partilha do conhecimento e a aprendizagem. A cultura organizacional tem um papel determinante na partilha do conhecimento e na definição de poderes.

É neste contexto que a Gestão de Incidentes pode contribuir com a detecção, registo e investigação de incidentes que podem auxiliar à mitigação de riscos, contribuindo para a inexistência de falhas parciais ou mesmo totais.

As políticas de gestão como incentivos ou recriminações às notificações de incidentes, assim como a atribuição de recursos apropriados às investigações destes, podem ter resultados surpreendentes e promissores espelhados neste trabalho, através do estudo de variáveis comportamentais de gestão num modelo de simulação dinâmica.

Palavras-chave: Segurança, Gestão de Incidentes, Informação, Risco, Sistemas Dinâmicos

Abstract

The purpose of this paper is to demonstrate that the policies of management in an organization can have a direct influence in the security of information, and that the technology by itself is not enough to provide an efficient means of protection.

In this sense, Knowledge Management can give a positive contribution, considering the evolution and the autonomy of the individuals that constitute the organization, stimulating the sharing of information, the sharing of knowledge and learning. The organizational culture has a decisive role in sharing the knowledge and defining powers.

It is in this context that Incident Management can contribute by detecting, registering and investigating incidents that might help minimizing risks and having a minimum of partial faults, or even total faults.

Management policies as incentives or recriminations of incidents notifications, along with the appropriate attribution of adequate resources when investigating them, can have surprising and promising results, as we show in this paper through the study of management behavioral variables in a model of dynamic simulation.

Keywords: *Security, Incidents Management, Information, Risk, Dynamic Systems*

Agradecimentos

À minha esposa Marina, por todo o apoio disponibilizado que permitiu uma dedicação incondicional à elaboração deste trabalho e aos meus filhos Daniel e David que compreenderam a ausência do pai.

Aos professores da FEUCP o meu reconhecimento, em especial aos professores Raquel César e Tito Santos Silva, orientadores deste trabalho, e aos colegas que contribuíram com o seu conhecimento para o meu enriquecimento técnico e humano.

Ao professor Finn Olav Sveen da Gjovik University College da Noruega por todo o suporte e apoio neste trabalho.

Índice

Índice de Tabelas

Índice de Figuras

Abreviaturas

Abreviaturas	**Descrição**
AC	Controlos Aplicacionais
AG	Anomalia Grave
AI	Aquisição e Implementação
BSI	*British Standards Institute*
CAA	*Civil Aeronautics Administration-Taiwan*
CERT	Serviço de Resposta a Incidentes de Segurança Informática
CIA-NR	Confidencialidade, Integridade, Disponibilidade e Não-Repudio
CMDB	*Change Management DataBase*
CobiT	*Control Objectives for Information and Related Technology*
COSO	*Committee of Sponsoring Organizations*
COSO ERM	*COSO Enterprise Risk Management*
DS	Entrega e Suporte
FCCN	Fundação para a Computação Científica Nacional
FEUCP	Faculdade de Engenharia Universidade Católica Portuguesa
IEC	Comissão Eletrotécnica Internacional
ISACA	*Information Systems Audit and Control Association*
ISIRT	*Information Security Incident Response Team*
ISO	Organização International de Normalização
ITIL	*Information Technology Infrastructure Library*
KGI	*Key Goal Indicator*
KPI	*Key Performance Indicator*
ME	Monitorização e Avaliação
MIT	*Massachusetts Institute of Technology*
NIST	*National Institute of Standards and Technology*
PDCA	*Plan-Do-Check-Act*

PC	Controlos de Processo
PO	Planeamento e Organização
RACI	Matriz de Atribuição de Responsabilidades (Responsável, Autoridade, Consultado, Informado)
RCTS	Rede Ciência, Tecnologia e Sociedade
RFC	*Request For Change*
SEI	*Software Engineering Institute*
SGSI	Sistema de Gestão de Segurança da Informação
SI	Sistemas de Informação
SLA	*Service Level Agreement* – Acordo de Nível de Serviço
SOA	*Statement of Applicability*
SW-CMM	*Capability Maturity Model for Software*
TI	Tecnologia de Informação
TIC	Tecnologias de Informação e Comunicação

1. MOTIVAÇÃO, OBJECTIVOS E METODOLOGIA

1.1. Motivação

A elaboração deste trabalho é motivada por uma questão que se coloca e à qual irei apresentar uma resposta:

Precisamos de sistemas de aprendizagem de incidentes na segurança da informação?

Muitas indústrias e empresas individuais têm implementado com sucesso sistemas de notificação de incidentes de segurança. A Norsk Hydro, uma das principais empresas norueguesas de energia, foi uma das primeiras a introduzir este tipo de sistemas com bons resultados (Jones et al., 1999). Nos últimos anos, a indústria dos cuidados de saúde viu uma "invasão" dos sistemas de notificação de incidentes de segurança, embora com resultados mistos (James, 2003; Nyssen et al., 2004; Stanhope et al., 1999). Mesmo assim, não há grandes dúvidas de que os sistemas de notificação de incidentes de segurança têm contribuído significativamente para uma melhoria da segurança.

Será um sistema de notificação que abrange toda uma organização, ou mesmo até toda uma indústria, necessário à implementação com sucesso da segurança da informação? Schneier (2000), numa frase apaixonada, compara a situação frustrante da notificação de dados da ciber-segurança com o sucesso dos sistemas de notificação da segurança aérea. Gonzalez (2005) oferece mais argumentos no sentido da necessidade de um tal sistema, dando enfoque à notificação de incidentes como um processo de melhoria de qualidade.

A necessidade da partilha de informação não é algo de desconhecido na área da informação de segurança. A implementação dos Centros de Análise e Partilha de Informação (ISACS) foi encorajada pelo governo americano (Gal-Or e Ghose, 2005). No entanto, existem obstáculos como a tendência das organizações para o "deixa-andar" (Gordon et al,. 2003) e incentivos distorcidos (Anderson, 2001), que surgem, entre outros factores, da descontinuidade entre as necessidades do negócio e a segurança.

Davenport e Pruzak (1998) falam dos mercados de conhecimento. Eles vêem a empresa como tendo um mercado interno de conhecimento, que consiste em vendedores, compradores e intermediários. A disponibilidade de um vendedor em partilhar informação depende de três condições: (1) Reciprocidade, ou seja, a expectativa de vantagens futuras na partilhar a informação agora. (2) Notoriedade, ou seja, tornar-se conhecido como alguém experiente, informado, e do estatuto que isso implica. (3) Altruísmo, ou seja partilhar só pelo desejo de ajudar. Ao alargarmos estes conceitos às interacções inter-organizacionais,

podemos inferir que as companhias não irão partilhar o seu conhecimento se não virem vantagem nisso. Além disso, é pouco provável que organizações comerciais partilhem o seu conhecimento por notoriedade ou altruísmo.

O estado da segurança da informação é relativamente imaturo quando comparado com o estado da segurança noutras industrias. No campo da segurança da industria, existem numerosos sistemas de notificação, frequentemente mandatados por lei, ou se não directamente por lei, por intensa pressão política. Talvez não vejamos sistemas de notificação de incidentes completamente funcionais antes de uma intervenção governamental, ou de uma ameaça de intervenção governamental.

Outra razão para uma adopção relativamente lenta dos sistemas de notificação de incidentes poderá ser o enfoque exclusivamente na segurança da informação como uma questão técnica. Os colaboradores não-técnicos são, frequentemente, mantidos completamente fora do ciclo e têm, pelo contrário, de usar um conjunto de regras pré-estabelecidas. Todavia, esta é uma abordagem limitada à formação dos utilizadores. *"... a regulação do comportamento depende de muitos outros aspectos, que não apenas da quantidade de formação dada ao utilizador*" (Görling, 2006). Os utilizadores têm de ser mantidos 'no ciclo'; só aí será evidente a necessidade e utilidade no cumprimento das regras definidas pelos especialistas da segurança da informação.

1.2. Objectivos

Esta dissertação tem como objectivo o estudo do efeito de certas variáveis de gestão no desempenho das organizações, ao nível da segurança da informação, medido pela taxa de ocorrência de incidentes. Para essa análise utiliza-se o modelo de eventos e incidentes de segurança da informação, que incorpora de forma quantitativa o efeito das políticas adoptadas pela gestão.

As variáveis de gestão analisadas reflectem políticas de incentivos adoptadas, empenho demonstrado pela gestão no tratamento dos eventos de segurança de informação e a atribuição de recursos competentes e com conhecimentos para investigar os eventos ou incidentes.

Ao nível das políticas de incentivos, procura-se avaliar os efeitos produzidos pela adopção de estratégias distintas no tratamento da notificação de incidentes, distinguindo entre políticas de recriminação de notificação de incidentes versus políticas de reforço positivo.

Neste sentido, usa-se um modelo dinâmico de gestão de incidentes que tem por base as normas e boas práticas da segurança de informação. É analisado o comportamento deste modelo sob a acção de variáveis exógenas que reflectem as variáveis de gestão em estudo,

procurando extrair conclusões sobre o principal impacto que estas variações podem gerar na segurança da informação.

1.3. Metodologia

A metodologia deste trabalho aborda a descrição de um processo de gestão de incidentes, representado num modelo dinâmico, ao qual vão ser adicionados cenários com variáveis que alteram os seus valores ao longo do tempo, apresentando no final gráficos com o comportamento dos vários cenários simulados. Esta simulação do modelo dinâmico será efectuada no software Vensim PLE, da Ventana Systems, INC.

Inicialmente o cenário irá ser focado com maior relevância pela gestão nos incidentes, com uma redução em 75% nas recriminações aos colaboradores que notificarem os incidentes, com efeito após o terceiro mês, variando seguidamente para um incremento em 75% dos incentivos de notificação de incidentes, com efeito após o terceiros mês. Será ainda analisado o cenário em que os recursos dedicados à investigação dos incidentes são reduzidos em 95% das necessidades de investigação.

Na sequência, a simulação focará a mesma importância dada pela Gestão entre os incidentes e os eventos, com uma redução em 75% nas recriminações aos colaboradores que notificarem os incidentes após o terceiro mês, variando seguidamente para um incremento em 75% dos incentivos de notificação de incidentes após o terceiros mês.

As variáveis exógenas que serão objecto de variação para este modelo são as seguintes:

- “Redução das Recriminações”;
- “Incremento dos Incentivos”;
- “Redução da Investigação”.

No final é efectuada uma análise entre os vários cenários e os seus resultados, apresentando as principais conclusões deste estudo. Neste sentido este trabalho encontra-se organizado em capítulos, apresentados na **Tabela 1.1** com a descrição do seu conteúdo.

Capítulo 1	**Neste capítulo é descrita a Motivação, assim como os Objectivos e a Metodologia deste trabalho**
Capítulo 2	**Neste capítulo é descrito o Estado da Arte.**
Capítulo 3	**Neste capítulo é descrito um Processo de Gestão de Incidentes e o correspondente mapeamento para o Modelo Dinâmico.**
Capítulo 4	**Neste capítulo são apresentados os resultados das simulações no Modelo Dinâmico.**
Capítulo 5	**Neste capítulo são apresentadas as Conclusões e o Trabalho Futuro.**
Capítulo 6	**Neste capítulo são apresentados os Anexos que suportam este trabalho.**
Capítulo 7	**Neste capítulo é apresentado o Glossário que suporta este trabalho.**
Capítulo 8	**Neste capítulo são apresentadas as Referências que suportam este trabalho.**

Tabela 1.1 – Capítulos e conteúdos.

A recolha bibliográfica incidiu sobre um conjunto de áreas que foram consideradas fundamentais para o tratamento e a compreensão do tema proposto, tendo sido abordado em primeiro lugar as questões que dizem respeito a definições e clarificação dos conceitos usados e uma abordagem das metodologias existentes de forma a poder efectuar uma selecção das mais relevantes.

Numa segunda fase da recolha bibliográfica, esta incidiu sobre as questões relacionadas com o papel dos sistemas de informação nas organizações e os aspectos relacionados com a necessidade de garantir o alinhamento entre o negócio com as TI/SI, maximizando os recursos e salvaguardando a informação da organização.

2. O ESTADO DA ARTE

2.1. Normas e Boas Práticas

2.1.1 Introdução

Este capitulo descreve o estado da arte no âmbito da gestão de incidentes, abordando as normas e boas práticas (*CobiT*, ITIL, ISO 27001, ISO 27002 e ISO 18044), existentes e em uso nas organizações, focando essencialmente o sector financeiro, apesar da grande importância que a gestão de incidentes têm noutros sectores, nomeadamente no sector alimentar. Este capítulo aborda ainda a dinâmica de sistemas como ferramenta para a modelação dinâmica de gestão de incidentes.

2.1.2. *CobiT*

O *Control Objectives for Information and related Technology* (*CobiT*), foi desenvolvido nos Estados Unidos da América em 1996 e tem como objectivo fornecer boas práticas através de um modelo de domínios e processos, apresentando actividades numa estrutura lógica de gestão. As boas práticas do *CobiT* representam o consenso dos especialistas, estando fortemente focadas mais nos controlos e menos na execução. Estas práticas são extremamente importantes pois são um auxiliar para a optimização dos investimentos em TI, garantido a entrega dos serviços e auxiliando com métricas para detectar os desvios.

Para a área de TI ter sucesso na entrega dos serviços solicitados pelo negócio, deve de implementar um sistema interno de controlos ou uma metodologia, com o objectivo de:

- Fazer uma ligação com os requisitos do negócio;
- Organizar as actividades de TI em um modelo de processos;
- Identificar os mais importantes recursos de TI;
- Definir os objectivos de controlo.

A orientação aos negócios do *CobiT* consiste em objectivos de negócio ligados a objectivos de TI, fornecendo métricas e modelos de maturidade para medir a sua eficácia e identificando as responsabilidades relacionadas dos donos dos processos de negócio e de TI.

O *CobiT* agrupa os processos de TI subdivididos em quatro domínios e 34 processos **(Anexo I)**, fornecendo assim uma visão total da área de TI:

- Planeamento e Organização (PO), com 10 processos;
- Aquisição e Implementação (AI), com 7 processos;
- Entrega e Suporte (DS), com 13 processos;
- Monitorização e Avaliação (ME), com 4 processos;

O modelo está representado na **Figura 2.1,** com o detalhe dos domínios e os seus respectivos processos.

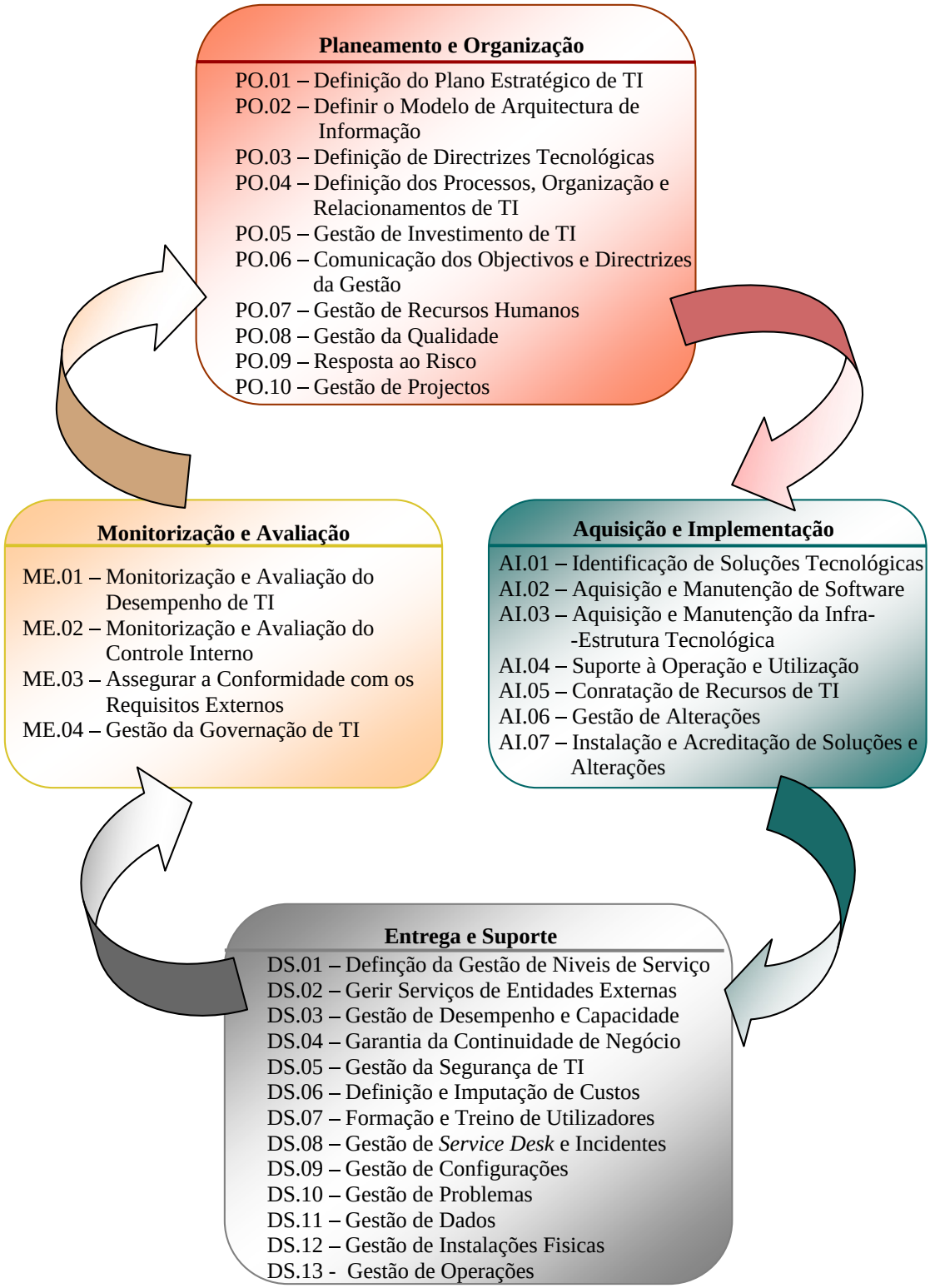


Figura 2.1 - Domínios do *CobiT* *(CobiT, 2007)*

A avaliação do processo de capacidade baseado nos modelos de maturidade do *CobiT* é uma parte fundamental da implementação da governação de TI. Depois de identificar os processos e os controlos críticos de TI, o modelo de maturidade permite a identificação das deficiências em capacidade e a sua demonstração para os gestores. Planos de acção podem ser desenvolvidos para elevar esses processos ao desejado nível de capacidade.

O *CobiT* suporta a governação de TI fornecendo uma metodologia para assegurar que:

- A área de TI esteja alinhada com o negócio;
- A área de TI habilite o negócio e maximiza os benefícios;
- Os recursos de TI sejam usados responsavelmente;
- Os riscos de TI sejam geridos apropriadamente.

A medição da performance é essencial para a governação de TI, incluindo a definição e a monitorização dos objectivos de medição sobre os quais os processos de TI precisam de entregar (processos de saída) e como entregam (processo de capacidade e performance). Muitas análises identificaram a falta de transparência dos custos, do valor e dos riscos de TI como uma das mais importantes para a governação de TI.

Todos os componentes do *CobiT* são interrelacionados, proporcionando o suporte para as necessidades de governação, gestão, controlo e avaliação conforme demonstrado na **Figura 2.2.**

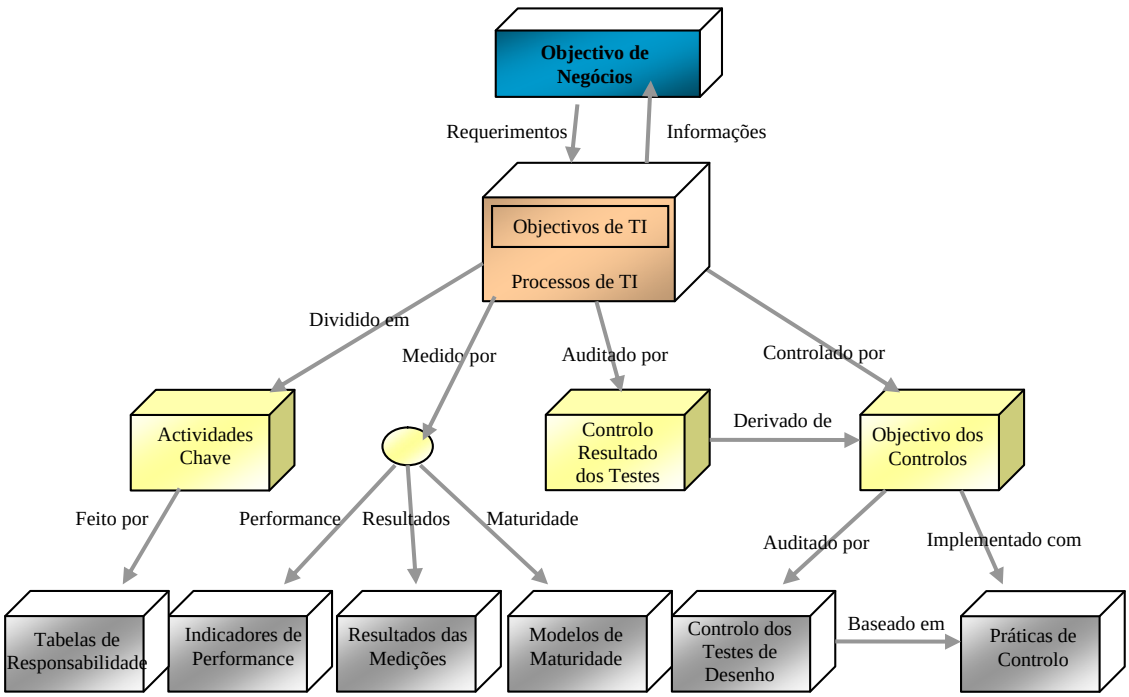


Figura 2.2 – Interrelacionamentos dos Componentes de CobiT

Os benefícios de implementar o *CobiT* como um modelo de governação de TI incluem:

- Um melhor alinhamento baseado no foco do negócio;
- Uma visão clara para os gestores sobre a realidade de TI;
- Uma clara divisão das responsabilidades baseada na orientação para processos;
- Aceitação geral por terceiros e entidades reguladoras;
- Compreensão por parte de todas as entidades envolvidas nos processos;
- Cumprimento dos requisitos do COSO para controlo do ambiente de TI;

O *CobiT* organiza-se por quatro domínios, 34 processos, 210 objectivos de Controlo e 990 práticas de controlo de TI (**Figura 2.3**).

Figura 2.3 – Relação entre processos e controlos no *CobiT*

2.1.2.1. Critérios de Informação do *CobiT*

Para atingir os objectivos de negócio, as informações precisam de se adequar a certos critérios de controlos, aos quais o *CobiT* denomina necessidades de informação da empresa. Baseado em abrangentes requisitos de qualidade, guarda e segurança, o *CobiT* assenta em sete critérios de informação distintos (**Anexo II**):

- **Efectividade** – Lida com a informação relevante e pertinente para o processo de negócio, garantindo a entrega atempada, de maneira correcta, consistente e utilizável;
- **Eficiência** – Relaciona-se com a entrega da informação através da optimização dos recursos;

- **Confidencialidade –** Está relacionada com a protecção de informações confidenciais, para evitar a divulgação indevida;
- **Integridade –** Relaciona-se com a fiabilidade e totalidade da informação bem como sua validade de acordo com os valores de negócio e expectativas;
- **Disponibilidade –** Relaciona-se com a disponibilidade da informação quando exigida pelo processo de negócio. Também está ligada à salvaguarda de recursos necessários e capacidades associadas;
- **Conformidade –** Lida com a conformidade legal, regulamentar e obrigações contratuais aos quais os processos de negócio estão sujeitos;
- **Fiabilidade –** Relaciona-se com a entrega da informação apropriada para os gestores gerirem a empresa;

2.1.2.2. Recursos de TI

Para satisfazer os requisitos de negócio para TI, a empresa precisa de investir nos recursos necessários para criar uma adequada capacidade técnica que satisfaça as necessidades de negócio, resultando no desejado retorno de negócio (incremento das vendas, etc).

Os recursos de TI identificados no *CobiT* são definidos da seguinte maneira:

- **Aplicações –** são sistemas automatizados utilizados pelos utilizadores, que processam os dados;
- **Informação –** são os dados em todas as suas formas, a entrada, o processamento e a saída fornecida pelo sistema de informação, em qualquer formato a ser utilizado pelo negócio;
- **Infra-estrutura –** refere-se à tecnologia e aos recursos (hardware, sistemas operativos, bases de dados, redes, etc), que possibilitam o processamento das aplicações;
- **Pessoas –** são os recursos necessárias para planear, organizar, adquirir, implementar, entregar, suportar, monitorizar e avaliar os sistemas de informação e serviços. Estes recursos podem ser internos, externos ou contratados, conforme as necessidades;

2.1.2.3. Inputs e Outputs do Processo Gerir o *Service Desk* e os Incidentes

As orientações de gestão fornecem, para cada processo de TI, *inputs* e *outputs* que permitem perceber os relacionamentos entre os processos. A **Figura 2.4** mostra, os relacionamentos do processo DS.08 – Gestão do *Service Desk* e Incidentes.

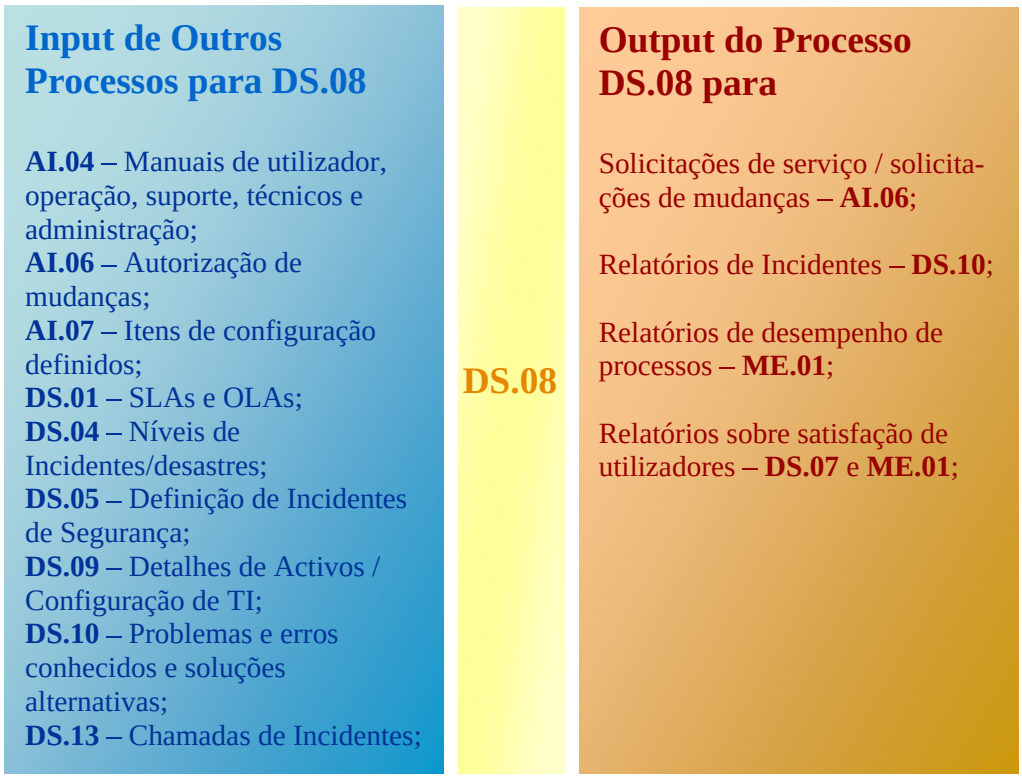


Figura 2.4 - Interfaces e/ou dependências do DS.08 com outros processos

2.1.2.4. Processo *CobiT* DS.08 – Gerir o *Service Desk* e os Incidentes

O processo *CobiT* DS.08 tem como objectivos primários a Eficácia e a Eficiência (**Figura 2.5**).

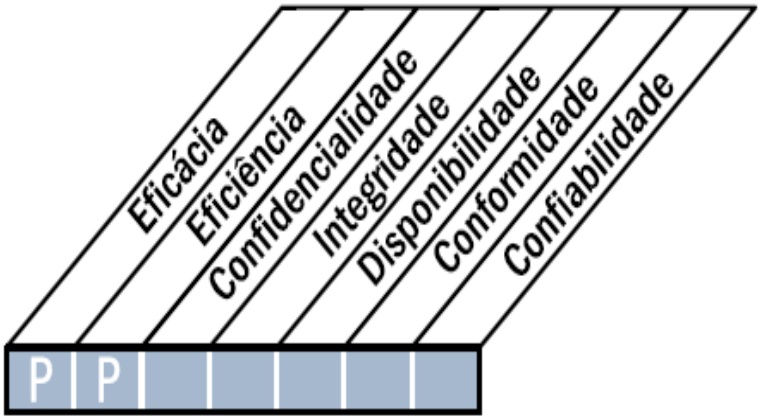


Figura 2.5 – Requisitos de negócio do Processo DS.08

A resposta efectiva e em tempo adequado a dúvidas e a problemas dos utilizadores de TI requer a existência de um *service desk* e um processo de gestão de incidentes bem projectados e implementados. Esse processo inclui a implementação de uma central de serviços com capacidade para o tratamento de incidente, incluindo o registo, encaminhamento, análise de tendências, análise de principais causas e resolução. Os benefícios ao negócio incluem o aumento de produtividade por meio de resolução rápida das chamadas reportadas pelos utilizadores. Complementarmente, as áreas de negócio podem tratar a origem das situações através de relatórios para análise e divulgação.

2.1.2.5. Controlo sobre o Processo de TI – DS.08 - Gerir o *service desk* e os incidentes

Que satisfaça os seguintes requisitos do negócio para a TI:

Permitir o uso eficaz dos sistemas de TI através de análise e resolução por consultas, solicitações e incidentes

Com foco em:

Prover um *service desk* profissional com respostas rápidas, procedimentos claros de escalonamento, análise de tendências e resolução **(Figura 2.6).**

É alcançado por:

- Instalação e operação de uma área de *service desk*;
- Monitorização e registo das tendências;

- Definição clara de critérios e procedimentos de escalonamento.

E medido por:

- Satisfação do utilizador com o primeiro nível de atendimento;

- Percentagem de incidentes resolvidos no tempo estipulado/aceitável;

- Índice de desistência das situações reportadas.

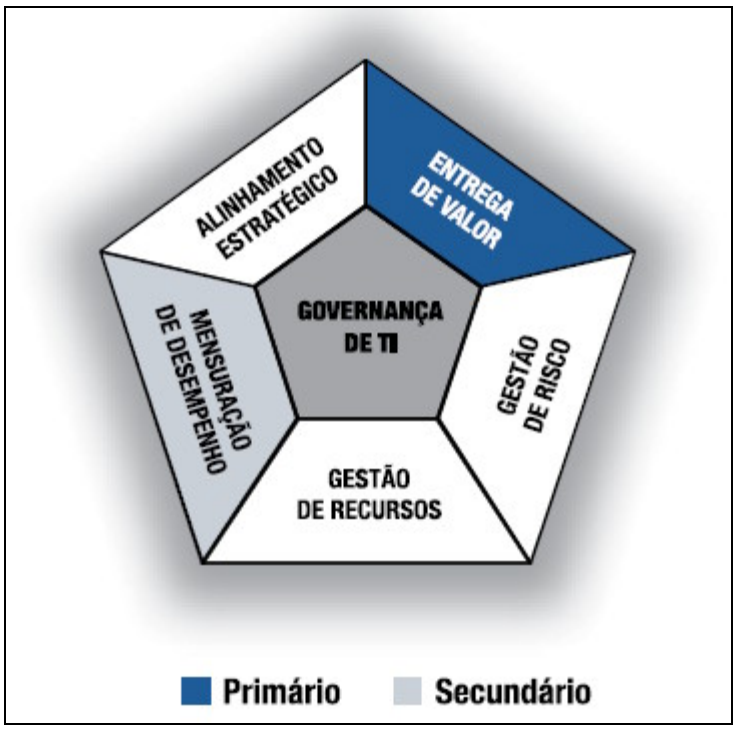


Figura 2.6 – Áreas de Foco do Processo DS.08

2.1.2.6. Objectivos de Controlo Detalhados

DS.08.1 *Service Desk*

Estabelecer um *Service Desk*, que é a ligação entre o utilizador e as TI, para registar, comunicar, analisar e resolver todos as situações, incidentes reportados, solicitações de serviços e procura de informação. Devem existir procedimentos de monitorização e encaminhamento com base em níveis de serviço acordados relativos ao SLA adequado que

permita a classificação e a prioritização de qualquer dúvida reportada como incidente, solicitação de serviço ou solicitação de informação. Medir a satisfação dos utilizadores finais com a qualidade do serviço prestado pelo *service desk* e os serviços de TI.

DS.08.2 Registo de chamadas dos utilizadores

Estabelecer uma função e um sistema que permita o registo e o acompanhamento das situações reportadas, incidentes, solicitações de serviços e necessidade de informações. Deve trabalhar de perto com o processo de gestão de incidentes, problemas, mudanças, capacidade e disponibilidade. Os incidentes devem ser classificados de acordo com as prioridades de negócio e serviço e direccionados à equipa adequada de gestão de problemas. Os clientes devem ser informados sobre o estado do seu problema.

DS.08.3 Encaminhamento de Incidentes

Estabelecer os procedimentos de *service desk* para que os incidentes que não podem ser resolvidos imediatamente sejam adequadamente encaminhados, conforme os limites definidos no Acordo de Níveis de Serviço, e soluções temporárias sejam implementadas, caso o possam ser feito. Assegurar que a propriedade e a monitorização do ciclo de vida do incidente permaneçam com o *service desk,* independentemente do grupo de TI que esteja a trabalhar na resolução.

DS.08.4 Encerramento de Incidentes

Estabelecer os procedimentos para monitorização periódica do encerramento dos incidentes. Quando o incidente foi resolvido, assegurar que o *service desk* regista as soluções adoptadas para a resolução e confirma se as acções adoptadas foram aceites pelo cliente. Deve ainda registar e relatar os incidentes não solucionados (erros já conhecidos e alternativas existentes) para fornecer informação visando o adequado gestão de problemas.

DS.08.5 Relatório e Analise de Tendências

Gerar relatórios de actividades do *service desk*, permitindo aos gestores medir o desempenho e o tempo de resposta dos serviços e identificar tendências ou problemas recorrentes, para que o serviço possa ser melhorado sempre.

2.1.2.7. Responsabilidades do Processo DS.08– Gerir o *Service Desk* e os Incidentes

Na **Tabela 2.1** são apresentadas as funções dos intervenientes no processo DS.08 e as actividades inerentes a estas, identificando quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado (I).

Actividades \ Funções	CEO	CFO	Executivo de negócio	CIO	Prop. do processo de negócio	Resp. por Operações	Resp. por Arquitectura	Resp. por Desenvolvimento	Resp. por Adm. de TI	PMO	Conform., Auditoria, Risco e Seg.	Gestor Incidentes/Serv. Desk
Criar processos de classificação (severidade e impacto) e escalação (funcional e hierárquica)				C	C	C	C	C	C		C	AR
Detectar e registar incidentes, solicitações de serviço e solicitações de informações												
Classificar, investigar e diagnosticar consultas				I		C	C	C			I	
Resolver, recuperar e fechar incidentes					I	R	R	R			C	
Informar utilizadores (por exemplo actualizações de status)				I	I							
Produzir relatórios de gestão	I			I	I	I			I		I	

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), Consultado (C) e/ou Informado (I)

Tabela 2.1 – Tabela RACI

2.1.2.8. Avaliação da maturidade do processo DS.08

Modelo de Maturidade - DS.08 **Gerir o *Service Desk* e os Incidentes**	
0 - N Existe	- Não existe suporte para resolver problemas e questões dos utilizadores. - Há uma completa falta do processo de gestão de incidentes. - A organização não reconhece que há uma questão a ser tratada.
1 - Inicial	- A gestão reconhece a necessidade de um processo sustentado por ferramentas e pessoas para responder a chamadas dos utilizadores e gerir a resolução de incidentes. - Não existe um processo padronizado e só é oferecido suporte reactivo. - A gestão não monitoriza os problemas, incidentes ou tendências. - Não existe um processo de encaminhamento que assegure que o problema será resolvido.
2 - Repetitivo	- Existe uma consciencialização organizacional da necessidade de um *Service Desk* e de um processo de gestão de incidentes. - A assistência está disponível de maneira informal por intermédio de elementos que têm conhecimento. - Existem algumas ferramentas comuns para auxiliar na resolução de incidentes. - Não existe formação e treino formal, não há procedimentos padrão e comunicados e as responsabilidades ficam a cargo de cada pessoa.

Modelo de Maturidade - DS.08 Gerir o *Service Desk* e os Incidente	
3 – Definido	- A necessidade de um *Service Desk* e de um processo de gestão de incidentes é reconhecida e aceite. - Os procedimentos foram padronizados e documentados e ocorrem treinos informais. - Fica a cargo das pessoas obter treino e seguir os padrões. - Consolidação de perguntas frequentes (FAQs) e directrizes de utilizadores são desenvolvidas, mas as pessoas devem procurá-las, mas podem não segui-las. - Chamadas e incidentes são rastreados manualmente e monitorizados individualmente, porém não existe um sistema de reporte formal. - A resposta em tempo adequando as chamadas e incidentes não é medida e os incidentes podem continuar sem solução. - Aos utilizadores foi comunicado sobre como e onde registar os problemas e incidentes.
4 – Gerido	- Existe um completo entendimento dos benefícios do processo de gestão de incidentes em todos os níveis da organização e a função de *service desk* foi estabelecida nas unidades organizacionais adequadas. - As ferramentas e técnicas são automatizadas com uma base de conhecimento centralizado. - Os profissionais de *service desk* interagem muito proximamente com os profissionais do processo de gestão de problemas. - As responsabilidades são claras e a efectividade é monitorizada. - Os procedimentos para comunicação, escalonamento e resolução de incidentes são estabelecidos e comunicados. - O pessoal do *service desk* é treinado e os processos são melhorados através do uso de software específico. - A gestão desenvolve métricas para medir o desempenho do *service desk.*

Modelo de Maturidade - DS.08 Gerir o *Service Desk* e os Incidente	
5 – Optimizado	- O *service desk* e o processo de gestão de incidentes são estabelecidos e bem organizados, com serviço voltado ao cliente por ter conhecimento, ter foco no cliente e ser útil. - Métricas são sistematicamente medidas e reportadas. - FAQs abrangentes e completas são parte integrante da base de conhecimento. - Há ferramentas que permitem os utilizadores fazerem o diagnóstico e a resolução de incidentes. - Os avisos são consistentes, e os incidentes são resolvidos rapidamente dentro de um processo de encaminhamento estruturado. - A gestão utiliza uma ferramenta integrada para as estatísticas de desempenho do processo de gestão de incidentes e *service desk*. - Os processos têm sido refinados ao nível das melhores práticas da indústria, com base nos resultados de análise de indicadores de performance, melhorias contínuas (*benchmarking*) com outras organizações.

Tabela 2.2 – Modelo de Maturidade do DS.08

2.1.3. ITIL

O ITIL (*Information Technology Infraestruture Library*) é um conjunto de boas práticas para o fornecimento de serviços de TI com qualidade e focados no cliente. O ITIL foi desenvolvido no final dos anos 80 pela CCTA (*Central Computer Telecommunications Agency*), mas actualmente é promovido pela OGC (*Office for Government Commerce*) que é um organismo público do Reino Unido. (Silva & Martins, 2008)

O ITIL é actualmente uma referência na gestão dos serviços de informática, revelando-se como essencial as relações entre Processos, Pessoas e Tecnologias, estando subdividido por disciplinas, que analisam especificamente uma dado tópico:

- **Service Management –** Gestão Integrada entre a visão de negócio e da tecnologia. Gere o serviço em duas vertentes:
    - **Service Delivery –** Estabelece processos que asseguram o fornecimento a clientes dos serviços adequados para o suporte ao negócio;
    - **Service Suporte –** Cobre os processos referentes a actividades diárias de manutenção e suporte associadas a provisões de serviços de TI.

- **Planning to Implement Service Management -** Planeia, implementa e gere os processos de Gestão de Serviços numa organização, relacionando-os com a mudança cultural e organizacional;

- **Security Management –** Aborda todas as questões relacionadas com a segurança da informação e dos serviços prestados;

- **ICT Infrastructure Management –** Gere a infra-estrutura de TI, indispensáveis à actividade da organização;

- **Business Perspective –** Garante o alinhamento do negócio e a prestação de serviços de TI;

- **Application Management –** Garante a gestão das aplicações que dão suporte ao negócio da organização.

O referencial ITIL tem como objectivo a descrição das práticas de Gestão de Serviços de TI que garantam:

- A disponibilidade de serviços de TI que sirvam os objectivos dos Clientes, com características de qualidade bem definidas, nomeadamente em termos de estabilidade e fiabilidade;

- A criação de uma relação de confiança entre o fornecedor de serviços de TI e os seus clientes, internos ou externos.

A Gestão de Serviços de TI visa assegurar que as necessidades de negócio da organização são suportadas por serviços de TI com:

- A qualidade necessária – apropriada às necessidades do negócio e documentada objectivamente em Acordos de Níveis de Serviço (SLA's);

- Com um custo adequado – negociado e acordado com o cliente, sustentado por processos de Gestão Financeira de TI que permitem a sua contabilização e controlo;

- Valor acrescentado – através de uma definição de funcionalidades e requisitos em que o fornecedor de serviços de TI procura activamente conhecer o contexto de negócio de cliente e encontrar a melhor forma de colocar ao serviço das necessidades desse cliente as capacidades e recursos de que dispõe.

Como resultado de uma Gestão de Serviços de TI alinhada com o ITIL é esperada uma melhoria na qualidade e alinhamento com o negócio dos serviços de TI disponibilizados, assim como a redução do custo global **(Figura 2.7)**. (Ruivo, 2010)

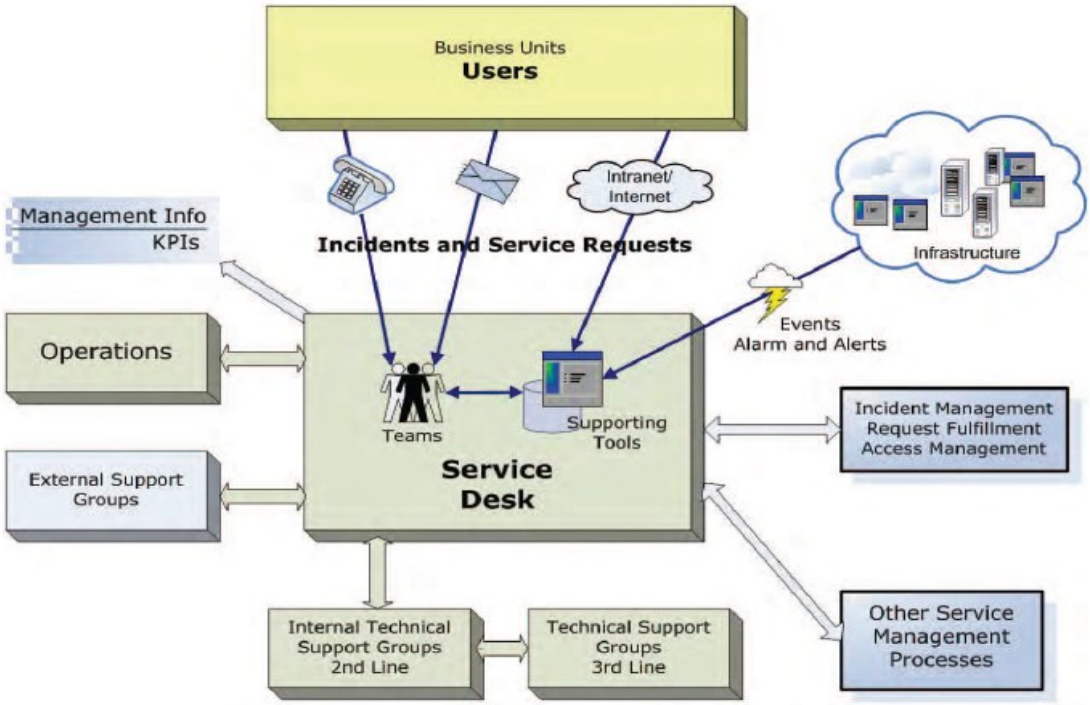


Figura 2.7- Service desk (Qualius)

No contexto deste trabalho, vamos analisar detalhadamente o Processo de Gestão de Incidentes com a abordagem do ITIL.

2.1.3.1. Gestão de Incidentes visto pelo ITIL

Definição

Um Incidente é qualquer evento que não faz parte do funcionamento standard de um serviço e que provoca ou pode provocar uma interrupção no serviço ou uma redução na respectiva qualidade. (Macfarlane, Rudd, 2001)

Objectivos

Repor o normal funcionamento do serviço tão rapidamente possível com o mínimo de interrupção do negócio, assegurando assim que os melhores níveis de disponibilidade e serviço pretendido são mantidos.

A Gestão de Incidentes permite:

- Assegurar a melhor utilização de recursos para apoiar o negócio;
- Desenvolver e manter registos significativos relativamente aos Incidentes;
- Definir e aplicar uma abordagem consistente a todos os Incidentes comunicados.

Exemplos de Incidentes:

- Aplicação indisponível aos clientes;
- Avaria ou limitação na utilização do equipamento;
- Bloqueio continuo da aplicação de negócio;
- Falha nas comunicações de dados.

Responsabilidades da Gestão de Incidentes:

- Detecção e registo de Incidentes;
- Classificação de todos os Incidentes e apoio inicial;
- Investigação e diagnóstico;
- Resolução e recuperação;
- Eliminação do Incidente;
- Propriedade, controlo, rastreio e comunicação do Incidente.

A **figura 2.8** apresenta o fluxo do ciclo de vida do incidente.

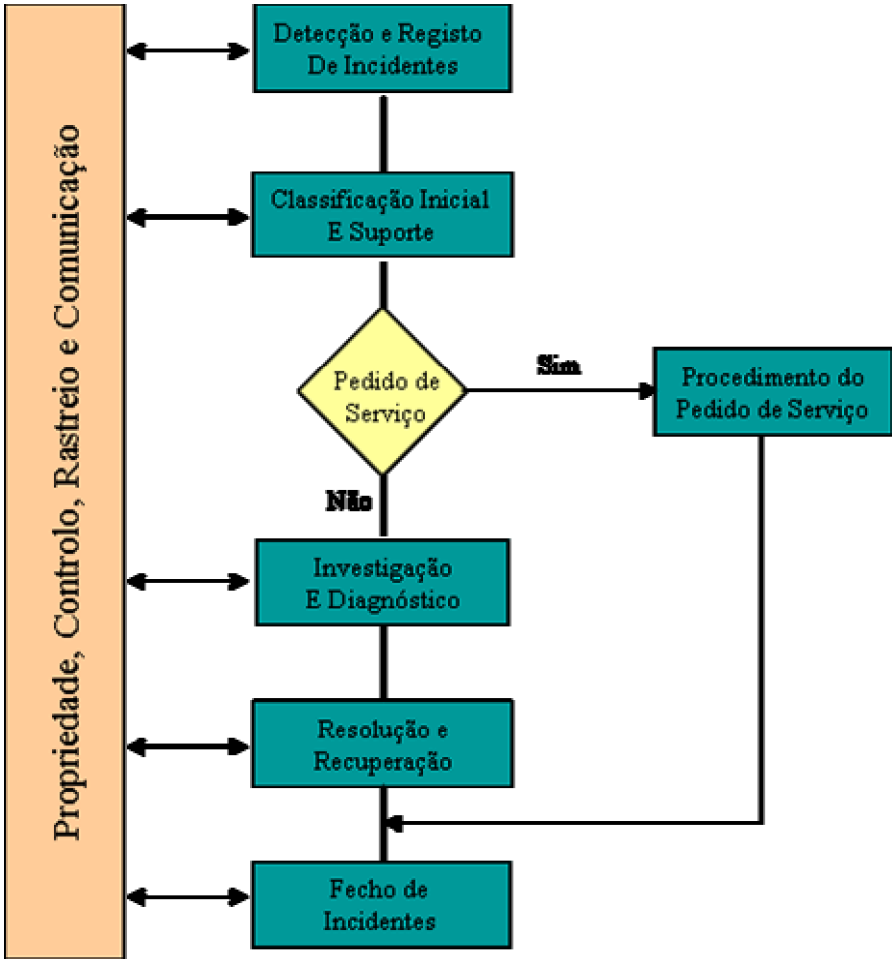


Figura 2.8 - O ciclo de vida do incidente

Factores de sucesso fundamentais na Gestão de Incidentes:

- Existência de uma base de dados de Gestão de Configurações (CMDB) actualizada;
- Existência de uma "base de conhecimento" com o registo dos dados dos problemas e dos erros conhecidos, resoluções e soluções;
- Disponibilização de ferramentas eficazes e automatizadas;
- Relacionamento estreito e efectivo com a Gestão de Níveis de Serviço.

A necessidade da Prioritização do Incidente

A prioridade para atribuição de recursos para resolução de um incidente é baseada numa combinação de impacto e urgência, em conjunto com outros factores relevantes, tais como a disponibilidade de recursos.

Urgência é uma avaliação da rapidez com a qual é necessário resolver um incidente e o impacto reflecte o efeito provável que o incidente terá sobre os serviços do negócio.

Relação entre Incidentes, Problemas e Erros Conhecidos

Nos casos em que um incidente não é identificável então, se houver investigação é criado um registo de Problema. Um problema apresenta um erro desconhecido num ou mais itens da configuração. Assim que a causa subjacente e uma correcção ou solução temporária estiverem identificadas, através de um pedido de alteração (*Request For Change*), o problema torna-se um registo de erro conhecido **(Figura 2.9)**. Os pormenores da relação entre incidentes, problemas, erros conhecidos e pedidos de alteração são incluídos numa CMDB (*Change Management Data Base*).

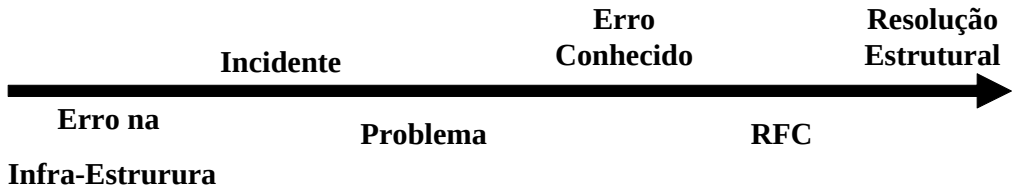


Figura 2.9 - Fluxo lógico do erro à resolução

Um problema é a causa subjacente desconhecida de um ou mais incidentes. O Problema passa a erro conhecido quando for descoberta a causa raiz e for identificada uma solução temporária ou uma alternativa permanente. (Macfarlane, Rudd, 2001)

Será efectuada uma correspondência entre os incidentes gravados recentemente e os incidentes, problemas e erros conhecidos, existentes na base de dados de conhecimento. Quando disponíveis, soluções temporárias serão aplicadas para permitir uma resolução rápida dos incidentes.

Os incidentes graves ocorrem quando o impacto nos utilizadores é muito forte ou quando se verifica um interrupção prolongada. A Gestão de Problemas deve ser notificada e marcar uma reunião formal com os elementos que possam ajudar a resolver e a ultrapassar a situação, devolver a normal operação aos sistemas.

Com a existência da Gestão de Incidentes podemos obter os seguintes benefícios:

- Redução do impacto no negócio, graças a uma resolução atempada dos incidentes;
- Identificação pró activa de melhorias vantajosas;

- Disponibilidade de Informações focadas no negócio relacionadas com o Acordo de Nível de Serviço (SLA);
- Melhor controlo do desempenho relativamente aos SLAs;
- Melhor utilização dos colaboradores resultando numa maior eficiência;
- Eliminação de Incidentes e pedidos de serviço perdidos;
- Informação mais precisa na CMDB, permitindo uma auditoria continua durante o registo de Incidentes;
- Melhor satisfação do Cliente e do Utilizador;
- Menor Interrupção para a equipa de suporte de TI e utilizadores.

2.1.4. Normas ISO 27001 e ISO 27002

2.1.4.1. Introdução

A norma ISO 27001 é um padrão reconhecido internacionalmente que apresenta os requisitos para um Sistema de Gestão de Segurança da Informação – SGSI (*Information Secutrity Management System – ISMS*), utilizando o modelo PDCA **(Anexo III).** Esta foi a primeira norma da série ISO 27000, a ser publicada pelo *International Organization for Standardization* (ISO), em Outubro de 2005.

A norma ISO 27001 é uma norma "standard" de segurança da informação, dedicada não só à segurança, mas também dedicada a aspectos e aos critérios específicos de auditoria operacional, não sendo uma norma técnica, ou um produto ou metodologia.

A norma ISO é a base para a gestão da segurança de informação, que todos que têm responsabilidades na segurança da informação deveriam usar.

2.1.4.2. História da ISO 27001

A ISO 27001 deriva do *British Standards Institute* (BSI) *Information Security Management* designada de norma BS 7799-2. A BSI tem sido pró activa na evolução da segurança da informação, respondendo às procuras da industria. Neste sentido nos anos 90 foi criado um grupo de trabalho dedicado à Segurança da Informação, culminando com um "Código de Boas Práticas de Gestão de Segurança da Informação" em 1993. Este trabalho originou a primeira versão da norma BS 7799 em 1995.

No final da década de 90, em resposta às exigências da indústria, a BSI formou um programa de acreditação de empresas de auditoria, ou entidades certificadoras com competências para

auditar a BS 7799. Simultaneamente foi constituído um comité de direcção, culminando com a actualização e actualização da BS 7799 em 1998, 1999, 2000 e finalmente em 2002.

Enquanto algumas organizações utilizaram a norma BS 7799, as necessidades foram aumentando, existindo a necessidade de criar um padrão internacionalmente reconhecido de segurança da informação, levando à actualização da BS 7799-2, e à publicação da ISO 27001 em Outubro de 2005 (ISO, 2005; Carlson, 2008).

2.1.4.3. Porquê a ISO 27001?

A segurança de informação tem sido tradicionalmente baseada nas "melhores práticas" e "orientações", contudo, está sujeita a várias interpretações e aplicações, nem sempre coerentes e harmoniosas, entre si.

A ISO 27001 oferece os seguintes benefícios:

- Um sistema de gestão reconhecido internacionalmente que pode aumentar a interoperabilidade da segurança da informação e confiança com terceiros;
- Um critério para avaliar a eficácia do Programa de Segurança da Informação;
- Um veículo para certificar vários regulamentos de protecção de dados.

(ISO, 2005; Carlson, 2008)

2.1.4.4. ISO 27001 versus ISO 27002

A **Tabela 2.3** apresenta as principais diferenças entre a norma ISO 27001 e a norma ISO 27002.

ISO 27001	ISO 27002
Uma norma de auditoria com base em requisitos auditáveis.	Um guia de execução, com base em sugestões de boas práticas.
Incide sobre os controlos de gestão que interessam às organizações.	Lista de controlos operacionais que uma organização deve considerar.
Usada para auditorias e para certificar Sistemas de Segurança de Informação em organizações.	Usada como meio de avaliação da abrangência dos Programas de Segurança Informática nas organizações.

Tabela 2.3 – Diferenças entre ISO 27001 e ISO 27002

(ISO, 2005; Carlson, 2008)

2.1.4.5. Áreas de controlo da ISO 27001

A ISO 27001 define um sistema de gestão de segurança da informação de acordo com a estrutura organizacional, com as politicas, com as actividades de planeamento, as responsabilidades, as práticas, os procedimentos, os processos e os recursos.

Define ainda um ISMS como parte do sistema global de gestão, baseado numa abordagem de risco, para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação. Essa abrangência faz com que esta norma favoreça a interacção entre departamentos da empresa e vários programas, tais como:

- Recursos Humanos;
- Jurídico;
- Auditoria;
- Instalações físicas;
- Continuidade de Negócios;
- Operações
- Segurança física.

Para cumprir este objectivo, a norma ISO 27001 identificou 5 áreas de controlo, 12 objectivos de controlo e 78 controles. Cada um é definido como um requisito sujeito a uma auditoria.

2.1.4.6. Capítulos da Norma ISO 27001

Nesta norma existem controlos que são abordados desde o capítulo 4 a 8 da norma, para que os sistemas de segurança das organizações estejam realmente em conformidade com a norma ISO 27001, que serão apresentados de seguida, destacando os capítulos com relevância.

A norma ISO 27001 é constituída pelos seguintes capítulos:

- 0 - Introdução;
- 1 - Âmbito;
- 2 - Referência Normativas;
- 3 - Termos e Definições da norma ISO 27001;
- 4 - Sistema de Gestão de Segurança da Informação.

  Este capítulo aborda a necessidade de estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um SGSI documentado, incluindo:

Criar e gerir o ISMS – Criação e gestão de risco de um processo baseado na:

- Definição do SGSI, incluindo áreas de actuação e limites;
- Identificação de activos de risco e metodologias de tratamento;
- Quadro de gestão para definir medição dos objectivos de controlo;
- Verificação do desempenho do ISMS.

(ISO, 2005; Carlson, 2008)

- 5 - Responsabilidade da Gestão.

  Este capítulo aborda as necessidades atribuídas às responsabilidades da gestão do ISMS, incluindo:

  - 5.1 Compromisso de Gestão – Identificação da gestão e comunicação de objectivos de segurança de informação em termos de tolerância ao risco.
  - 5.2 *Resource Management* – Fornecimento de recursos adequados para atender aos objectivos de controlo definidos e garantir a competência na execução dos mesmos.

  (ISO, 2005; Carlson, 2008)

- 6 - Auditorias Internas de um ISMS.

  Este capítulo aborda as necessidades de auditorias internas num ISMS, incluindo um procedimento de auditoria documentado, critérios de auditorias, frequência de actuações, metodologia e responsabilidades.

  (ISO, 2005; Carlson, 2008)

- 7 - Gestão de revisão de ISMS.

  Este capítulo aborda a necessidade de participação de gestão e apoio do ISMS, a saber:

  - 7.1 Geral – Revisões periódicas programadas e documentadas do desempenho do ISMS;
  - 7.2 Revisão de entradas – as diversas fontes e métricas necessárias para uma analise da gestão global;
  - 7.3 Revisão de saída – a gestão de vários critérios de revisão e decisão e a necessidade de controlar as alterações resultantes destas decisões de gestão.

(ISO, 2005; Carlson, 2008)

- 8 - Melhoramento do ISMS.

  Este capítulo aborda a necessidade da existência de mecanismos para melhorar continuadamente o ISMS, nomeadamente:

  - 8.1 Melhoria continua – Ferramentas e técnicas para medir e vigiar o desempenho do SGSI;
  - 8.2 A acção correctiva – Identificação reactiva e análise de causa de não--conformidades existentes no ISMS, bem como acompanhamento das soluções;
  - 8.3 Acção preventiva – A identificação pró activa e análise de causa de potenciais problemas com o ISMS, bem como acompanhamento das acções de alinhamento.

  (ISO, 2005; Carlson, 2008)

2.1.4.7. A Norma ISO 27002

A norma ISO 27002 fornece boas práticas para implementar o Sistema de Gestão de Segurança de Informação, sendo um documento de aconselhamento genérico que tem um âmbito alargado e requer adaptação a cada organização. Esta norma está organizada em 15 capítulos **(Figura 2.10)**, indica 39 objectivos de controlo e controlos a implementar.

Figura 2.10 - Hierarquização dos capítulos da norma ISO 27002

A norma ISO 27002 é constituída pelos seguintes capítulos:

- 1 - Introdução;
- 2 - Âmbito;
- 3 - Definições;
- 4 - Avaliação e Gestão de Risco;
- 5 - Política de Segurança;
    - 5.1 - Política de segurança da Informação;
- 6 - Organização de Segurança;
    - 6.1- Organização Interna;
    - 6.2 - Segurança nos acessos de terceiros;
- 7 - Gestão de Activos;
    - 7.1 - Responsabilidade pelos activos;
    - 7.2 - Classificação de informação;
- 8 - Segurança de Recursos Humanos;
    - 8.1 - Definição de funções de segurança;
    - 8.2 - Procedimentos de admissão;
    - 8.3 - Procedimentos de saída ou mudança de funções;
- 9 - Segurança Física;
    - 9.1 - Áreas de segurança;
    - 9.2 - Segurança do equipamento;
- 10 - Gestão de Comunicações e Operações;
    - 10.1 - Procedimentos operacionais e responsabilidades;
    - 10.2 - Gestão de serviços prestados por terceiros;
    - 10.3 - Planeamento de sistemas;
    - 10.4 - Protecção contra software malicioso;
    - 10.5 - Salvaguarda de dados e *logging*;
    - 10.6 - Gestão de redes;
    - 10.7 - Manuseamento e segurança de *media*;
    - 10.8 - Troca de informação com entidades externas;
- 11 - Controlo de Acessos;

- 11.1 - Requisitos de negócio para controlo de acessos;
- 11.2 - Gestão de acessos dos utilizadores;
- 11.3 - Responsabilidades dos utilizadores;
- 11.4 - Controlo de acessos à rede;
- 11.5 - Controlo de acessos ao sistema operativo;
- 11.6 - Controlo de acessos a aplicações;
- 11.7- Computadores móveis e tele-trabalho;

- 12 - Aquisição, Desenvolvimento e Manutenção de SI;
  - 12.1 - Requisitos de segurança de sistemas;
  - 12.2 - Segurança de aplicações;
  - 12.3 - Controlos criptográficos;
  - 12.4 - Segurança de ficheiros;
  - 12.5 - Segurança nos procedimentos de desenvolvimento e suporte;
- 13 - Gestão de Incidentes de segurança da informação;
  - 13.1 - Notificação de eventos e vulnerabilidades de segurança da informação.
    - 13.1.1 - Notificação de eventos de segurança da informação;
    - 13.1.2 - Notificação de vulnerabilidades de segurança da informação;
  - 13.2 - Gestão e melhoramentos dos incidentes de segurança da informação.
    - 13.2.1 - Procedimentos e responsabilidades;
    - 13.2.2 - Aquisição de conhecimento com os incidentes de segurança da informação;
    - 13.2.3 - Recolha de evidencias;
- 14 - Gestão de Continuidade de Negócio;
  - 14.1 - Aspectos de gestão da continuidade do negócio;
- 15 - Conformidade.
  - 15.1 - Conformidade com a lei;
  - 15.2 - Revisão da política de segurança;
  - 15.3 - Auditabilidade dos sistemas.

2.1.5. Norma ISO 18044

2.1.5.1. Introdução

Nenhuma politica de protecção ou de segurança de informação poderá garantir a protecção total da informação, dos sistemas de informação, serviços ou redes. Depois da implementação de todas as medidas de segurança, existe sempre um risco residual que permanece e que no decorrer do tempo pode tornar ineficaz as medidas de protecção de informação e, assim, originar incidentes de segurança de informação com impactos directos ou indirectos para o negócio da organização. Além disso, inevitavelmente, novas ameaças não identificadas anteriormente poderão surgir. A preparação insuficiente de uma organização para lidar com tais incidentes fará com que não exista uma resposta eficaz e firme e, potencialmente, vais aumentar o grau de adversidades criando impacto na organização e no negócio. Neste sentido é essencial para qualquer organização uma abordagem estruturada e planeada no sentido de (**Anexo IV**):

- Detectar, comunicar e avaliar incidentes de segurança de informação;
- Responder a incidentes de segurança de informação, nomeadamente através da activação de medidas adequadas de protecção, com a redução e recuperação de impactos;
- Aprender com os incidentes de segurança de informação, melhorando de forma contínua a gestão de incidentes de segurança de informação.

A **Figura 2.11** apresenta os fluxos e as tarefas de cada actividade apresentada pela norma ISO 18044, num processo muito similar ao ciclo PDCA (Plan, Do, Check; Act) (ISO, 2004)

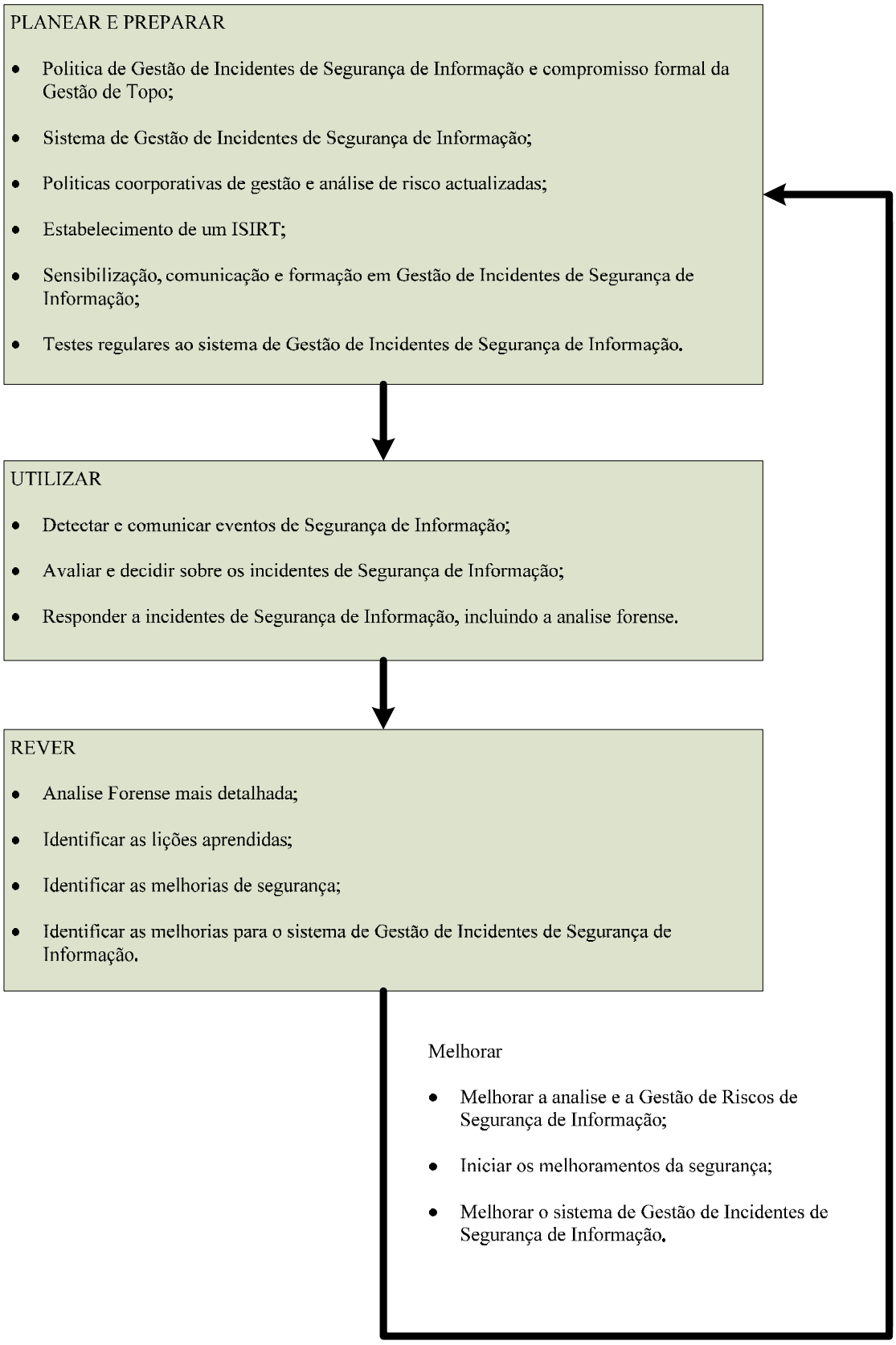


Figura 2.11 - Fluxos e tarefas da Gestão de Incidentes (ISO 18044, 2004)

A norma ISO 18044 é uma norma "standard" de Gestão de Incidentes de Segurança de Informação, estabelecendo boas práticas na implementação da Gestão de Incidentes numa organização.

A norma ISO 18044 é constituída pelos seguintes capítulos:

- 1 - Âmbito;
- 2 - Referências de normativos;
- 3 - Termos e definições;
    - 3.1 - Plano de Continuidade de Negócio;
    - 3.2 - Evento de Segurança de Informação;
    - 3.3 - Incidente de Segurança de Informação;
    - 3.4 - ISIRT (*Information Security Incident Response Team*);
    - 3.5 - Outros termos e definições;
- 4 - Conhecimento;
    - 4.1 - Objectivos;
    - 4.2 - Processos;
- 5 - Benefícios e Questões Chave;
    - 5.1 - Benefícios;
    - 5.2 - Questões chave;
- 6 - Exemplos de Incidentes de Segurança da Informação e suas causas;
    - 6.1 - Negação de Serviço;
    - 6.2 - Recolha não autorizada de informação;
    - 6.3 - Acesso não autorizado;
- 7 - Planear e Preparar;
    - 7.1 - Visão Global;
    - 7.2 - Politica de Gestão de Incidentes de Informação;
    - 7.3 - Programa de Gestão de Incidentes de Informação;
    - 7.4 - Politicas de Gestão de Risco de Segurança de Informação;
    - 7.5 - Constituição do ISIRT (*Information Security Incident Response Team*);
    - 7.6 - Suporte técnico e outros;
    - 7.7 - Conscencialização e treino;

- 8 - Usar;
    - 8.1 - Introdução;
    - 8.2 - Visão Global dos Processos Chave;
    - 8.3 - Detectar e Reportar;
    - 8.4 - Avaliação e Decisão de Eventos/Incidentes;
    - 8.5 - Respostas;
- 9 - Rever;
    - 9.1 - Introdução;
    - 9.2 - Apoiar a Analise Forense;
    - 9.3 - Lições Aprendidas;
    - 9.4 - Identificação de Melhorias de Segurança;
    - 9.5 - Identificação de Melhorias de Esquemas;
- 10 - Melhorar;
    - 10.1 - Introdução;
    - 10.2 - Melhorias na analise e gestão de Riscos de Segurança;
    - 10.3 - Efectuar melhorias de Segurança;
    - 10.4 - Efectuar melhorias no Programa de Gestão de Incidentes;
    - 10.5 - Outras melhorias.
- 11 - Sumário.

2.1.6. Conclusão

Nas secções anteriores foram apresentadas as normas e boas práticas com áreas de relevo na gestão de incidentes. Contudo em todas elas existem sobreposições nesta matéria, estando em curso investigação sobre o problema de conciliar todas essas normas e boas práticas, sendo um problema em aberto.

2.2. A Gestão de Incidentes na Industria

2.2.1. Sector Financeiro

O *CobiT* Control Practices – *Guidance to Achieve Control Objectives for Successful IT Governance*, contém a informação necessária para que as organizações adaptem a *framework* de governação e controlo que o *CobiT* propõe.

A avaliação do *gap* entre as boas práticas proposta pelo *CobitT* e as práticas de controlo adoptadas pela Organização, depois de confirmada a conformidade dos controlos implementados, permite avaliar a sua maturidade.

O Basileia II define maturidades objectivo para as organizações financeiras conforme os indicados na **tabela 2.4**:

Domínio	Processo	Maturidade objectivo para Basileia II
PO	PO1	**3**
	PO2	**4**
	PO3	**3**
	PO4	**4**
	PO5	**3**
	PO6	**4**
	PO7	**3**
	PO8	**3**
	PO9	**4**
	PO10	**3**
AI	AI1	**4**
	AI2	**4**
	AI3	**4**
	AI4	**3**
	AI5	**3**
	AI6	**4**
	AI7	**4**

DS	DS1	**3**
	DS2	**3**
	DS3	**4**
	DS4	**4**
	DS5	**4**
	DS6	**3**
	DS7	**4**
	DS8	**4**
	DS9	**3**
	DS10	**4**
	DS11	**4**
	DS12	**4**
	DS13	**4**
ME	ME1	**3**
	ME2	**4**
	ME3	**4**
	ME4	**3**

Tabela 2.4 - Valores propostos por Basileia II

Este último valor é muito relevante para as organizações do sector financeiro, pois existe uma relação directa entre a maturidade das TI e o nível de reservas financeiras exigido pelo Banco de Portugal. Da análise dos resultados apresentados na **Tabela 2.4**, a Gestão recolhe informação que lhe permite decidir sobre quais os processos onde deve fazer um maior esforço na melhoria da maturidade. Este esforço deve incidir nos processos onde seja maior a exigência de Basileia II e onde seja maior o diferencial entre esse valor e o valor médio obtido na avaliação.

O objectivo do Acordo Basileia II é introduzir práticas robustas de gestão do risco de crédito e operacional e fortalecer a ligação entre risco e o custo do capital. Os seus regulamentos fornecem um incentivo para as organizações melhorarem a qualidade das suas *frameworks* de gestão de risco e dos sistemas, para reduzir o capital exigido. Esta melhoria fornece uma

vantagem competitiva para as organizações financeiras (Basel Committee on Banking Supervision, 2010).

Podemos verificar a grande importância dada à Gestão de Incidentes para o sector financeiro, uma vez que o Basileia II define como nível de maturidade objectivo dos mais elevados de todos os processos *CobiT* (DS.8 – Nível Objectivo de 4).

2.2.2. Sector alimentar

Cabe à indústria deste sector cumprir com todos os requisitos legais de forma aos consumidores a disponibilização de produtos alimentares em perfeitas condições de higiene, segurança, e qualidade. No entanto, mesmo quando são tomadas as devidas precauções, podem surgir falhas inadvertidamente, cujo as causas vão desde problemas de fabrico a erros na rotulagem que, na pior das hipóteses, poderão pôr em risco a saúde pública. Nesta situação a solução é actuar o mais rápido possível e responder com as acções correctivas necessárias para proteger os consumidores e, ao mesmo tempo, a reputação da empresa e/ou das marcas.

A Gestão de Incidentes e de crise faz, ou tem de fazer, hoje parte das estratégias de gestão de qualquer empresa do sector alimentar, porque ninguém está imune a que algo aconteça, porque é obrigatório pensar o impensável, porque não é possível ficar à mercê do improviso quando se trata da credibilidade e sobrevivência das organizações. E saber comunicar uma crise quando ela acontece é também um imperativo, pois será a melhor forma de a controlar e de não dar espaço a possíveis especulações e pânicos infundados, destacando no apoio da gestão de incidentes os seguintes processos: (Vargues, 2007)

- Sistemas de Respostas;
- Gestão de Equipas;
- Comunicação Externa;
- Prevenção e Planeamento.

No caso de um incidente de segurança alimentar, os produtores e distribuidores de produtos alimentares devem de actuar rapidamente de modo a aperceberem-se da natureza do problema e tomar acções correctivas necessárias para proteger a saúde dos consumidores e a reputação da empresa ou da marca. As acções a serem tomadas podem ir desde a cessação das vendas, bloqueio dos produtos na cadeia de abastecimento ou proceder a uma recolha pública dos produtos directamente do consumidor. Em qualquer dos casos devem ser

tomadas medidas com vista a eliminar as causas do problema e prevenir novas ocorrências. Além disso, uma boa colaboração entre autoridades competentes, a indústria e os meios de comunicação é de particular relevância para proteger os interesses de todas as partes envolvidas.

Para a gestão de um sistema de incidentes é essencial ter implementado procedimentos claros com responsabilidades bem definidas. Deve ser nomeado um Comité de Gestão de Incidentes multidisciplinar, de modo que possa tratar de grande variedade de potenciais assuntos. A primeira parte e mais difícil de qualquer incidente emergente é estabelecer a natureza e a extensão precisa do problema.

Os incidentes classificam-se como:

- Incidente de Segurança Alimentar (a segurança do consumidor está em risco);
- Incidente Legal (o produto não cumpre com um requisito legal, mas a segurança do consumidor não está em comprometida);
- Incidentes de Qualidade (a segurança do consumidor não está em risco, mas o produto está fora das especificações, não correspondendo às expectativas deste).

Dependendo da classificação do incidente e da análise de risco, a acção a ser tomada pode ir desde um bloqueio na distribuição do produto a uma recolha pública deste ao nível do consumidor (com a respectiva correcção do processo / produto / rotulagem pelo produtor). As combinações típicas de classificação são as seguintes:

- **Um Incidente de Segurança** de um produto, conduz a uma recolha do produto, sendo requerida quando este tem muitas probabilidades de causar sérios problemas para a saúde pública ou até mesmo a morte;
- **Um Incidente Legal** conduz a um bloqueio e / ou recolha do produto, sendo requerida quando o defeito que este apresenta não causar problemas nem consequências para a saúde dos consumidor, mas viola a legislação;
- **Um problema de Qualidade** conduz a um bloqueio e / ou recolha do produto, sendo neste caso uma acção voluntária para proteger uma marca ou a reputação da empresa, quando este é distribuído e não está em conformidade com as especificações ou com as expectativas do consumidor, sem contudo apresentar qualquer risco de segurança para o consumidor ou violação dos requisitos legais. As acções tomadas (bloqueio ou recolha – "pública" ou "silenciosa") deverão estar em linha com os possíveis prejuízos causados.

O alcance de qualquer acção para bloquear/recolher o produto pode ser efectuado a vários níveis:

- **Nível Interno:** Os produtos a serem bloqueados/recolhidos estão ainda dentro do controlo do produtor, possivelmente ainda na fábrica, em trânsito ou nos armazéns da empresa, mas ainda não estão no distribuidor ou no retalho;
- **Nível do mercado:** O produto em questão está no mercado retalhista, é então bloqueado/recolhido dos armazéns e muitas vezes das prateleiras dos retalhistas, geralmente de uma forma "silenciosa". É um caso típico de um incidente legal ou de qualidade;
- **Nível Público:** A recolha é feita até ao nível do consumidor, sendo requerida quando o incidente se supõe ser um problema de segurança e o público deve ser notificado para prevenir o consumo ou uso do mesmo.

O Comité de Gestão de Incidentes constituído por elementos com diferentes funções na empresa deve gerir qualquer problema com os produtos, de forma a assegurar um procedimento de bloqueio/recolha controlado. Todos os intervenientes devem de ser adequadamente treinados nos procedimentos de gestão de incidentes e acções relacionadas. (Cruz , 2006)

2.2.3. O CERT – Serviço de Respostas a Incidentes de Segurança Informática

2.2.3.1. Introdução

As novas tecnologias de informação e comunicação (TIC) tornaram-se numa infra-estrutura verdadeiramente crucial de suporte às actividades no nosso quotidiano. Temos vindo a assistir a uma crescente dependência das TIC da parte dos vários sectores da nossa sociedade, de onde resulta que uma efectiva securização desta infra-estrutura, à semelhança de outras já consideradas críticas como as redes de distribuição de energia eléctrica ou a rede telefónica pública, se revista da maior importância.

Esta securização apresenta desafios de variada ordem. A combinação entre a quantidade de informação ligada em rede e a crescente complexidade dos sistemas computacionais e das aplicações que a trata tem vindo a tornar estes sistemas e a informação neles contida em alvos extremamente vulneráveis a ataques.

No dia 2 de Novembro de 1988 a Internet foi alvo de um software malicioso do tipo habitualmente designado por "*worm*". Este programa informático, criado por Robert Morris com o propósito de se auto-propagar através da rede, foi responsável pela contaminação de mais de 60,000 computadores, afectando negativamente e durante vários dias diversos serviços e a funcionalidade global da Internet. A rapidez de propagação e o consequente impacto do agora designado Morris Worm apanhou a então pequena comunidade Internet

desprevenida. Da análise do incidente verificou-se que o que mais prejudicou o normal funcionamento da rede e serviços associados não foi o tempo necessário para encontrar um antídoto eficaz, mas sim a inexistência de uma estrutura organizada que permitisse informar a comunidade da existência do incidente, efectuar uma eficaz distribuição do antídoto e instruir os utilizadores sobre a sua aplicação. Como consequência imediata foi então criado um centro de coordenação de resposta a incidentes de segurança designado de CERT/CC.

Outro exemplo ilustrativo da capacidade de destruição e impacto na vida dos cidadãos provocado por um incidente de segurança informática remonta a 2003. O worm sapphire ou SQL/Slammer, considerado ainda como o mais rápido até ao momento, atingiu 90% dos servidores SQL em todo o mundo em cerca de 10min., provocando a quebra total, entre outros, das redes de comunicação móvel na Coreia do Sul, da rede de terminais ATM do Bank of America, de 5 root servers DNS mundiais e do sistema de emissão de passagens aéreas da Continental Airlines. Em Portugal, 300.000 clientes ficaram privados, durante 12h, do serviço de Internet por cabo. Neste caso, a vulnerabilidade explorada era conhecida há mais de 6 meses e a rápida aplicação do "remendo" de software existente permitiu controlar a situação.

Mais recentemente, entre Abril e Maio de 2007, vários servidores Internet governamentais, fornecedores de serviço Internet, servidores de banca electrónica, portais de empresas de media e rede de pagamentos electrónicos na Estónia foram alvo de uma sequência de ataques, maioritariamente do tipo *Distributed Denial of Service* (DDoS), com resultados devastadores para a o normal funcionamento de um país por muitos considerado como um exemplo de vanguarda tecnológica.

Estes e outros incidentes de grande dimensão têm vindo a demonstrar as fragilidades de uma infra-estrutura considerada crítica no suporte a actividades que percorrem todos os sectores da sociedade. Por outro lado, a tendência observada nos últimos anos indica que os grandes incidentes de segurança das redes e da informação são suportados em estruturas profissionais (eg. RBNET, Intercage) que visam o ganho financeiro dos seus autores.

Os serviços de resposta a incidentes de segurança informática (CSIRTs) têm sido apontados como essenciais na prevenção e reacção a este tipo de fenómeno. Neste contexto, a FCCN, através do seu serviço CERT.PT, apresenta uma longa experiência a nível nacional e internacional, quer no tratamento e na coordenação da resposta a incidentes, quer na divulgação e outras formas de promoção do conceito CSIRT dentro do território nacional.

A nível nacional o CERT.PT tem vindo a promover a criação de novas CSIRT facilitando acções de formação e dando o apoio necessário ao seu estabelecimento. Como resultado a

FCCN tem vindo a assinar protocolos de cooperação com os principais operadores de telecomunicações e outras entidades relevantes com vista à criação de uma rede nacional de CSIRTs e cooperação efectiva nas áreas da segurança informática. A nível internacional, o serviço CERT.PT tem participado activamente nos principais *fora* relacionados com as temáticas da segurança informática e da gestão de incidentes e foi a primeira equipa de resposta a incidentes de segurança informática nacional a obter a acreditação internacional do serviço Trusted Introducer ainda em 2004. (CERT.PT, 2010)

2.2.3.2. Missão

O CERT.PT tem como missão contribuir para o esforço de cibersegurança nacional nomeadamente no tratamento e coordenação da resposta a incidentes, na produção de alertas e recomendações de segurança e na promoção de uma cultura de segurança em Portugal. Para esse efeito:

- Presta apoio a utilizadores de sistemas informáticos na resolução de incidentes de segurança, aconselhando procedimentos, analisando artefactos e coordenando acções com as entidades envolvidas;
- Reúne e dissemina informação relacionada com novas vulnerabilidades de segurança e produz recomendações referentes a potenciais riscos de segurança e actividades maliciosas em curso no sentido de formar uma consciência de segurança junto dos utilizadores de sistemas informáticos;
- Promove a criação de novos CSIRT em Portugal e a cooperação entre estes.

O CERT.PT responde a incidentes de segurança informática no contexto da comunidade utilizadora da RCTS - Rede Ciência, Tecnologia e Sociedade **(Figura 2.12)**.

Adicionalmente presta o serviço de coordenação da resposta a incidentes dentro do território nacional e em particular para os CSIRT com os quais tem acordos celebrados.

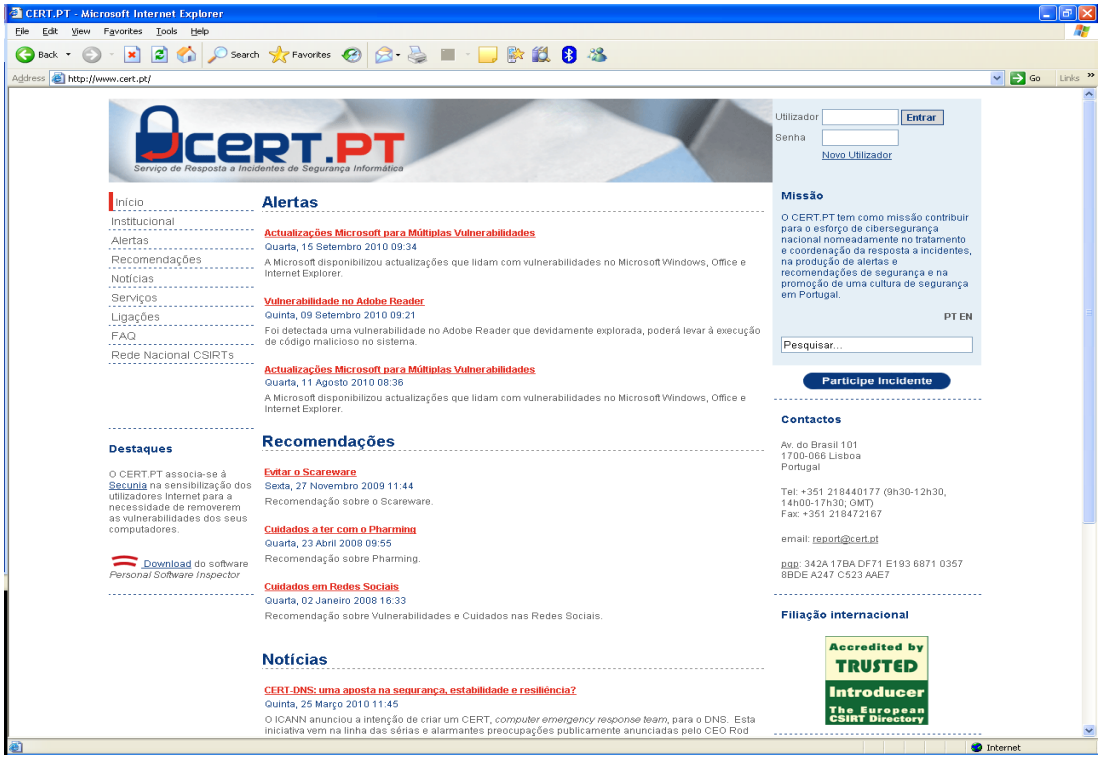


Figura 2.12 – Sítio do CERT.PT na internet

2.3. Sistemas Dinâmicos

2.3.1. Introdução

Os Sistemas Dinâmicos surgiram como uma metodologia de simulação de variáveis da gestão, criada em 1958 por o Professor Dr. Jay W. Forrester, engenheiro e investigador do MIT – Massachusetts Institute of Technology e cujo o objectivo era apoiar o processo de tomada de decisão, verificando os desvios entre o comportamento da realidade e o previsto, por meio de um processo de aprendizagem sobre um determinado contexto, com o objectivo de compreendê-lo e permitir acção sobre os mesmo. Esta área do conhecimento deriva da escola do pensamento sistémico e propõe-se a apresentar os contextos pela representação dos seus eventos. Este método identifica as variáveis e os factores críticos do referido contexto, delineando padrões de comportamento e representando a sua estrutura sistémica para que se possam aplicar arquétipos preconcebidos. Esses arquétipos são comportamentos observados sistematicamente definidos em razão da complexidade do mapeamento do contexto. A resultante do método passa pela identificação de modelos mentais que podem ser reavaliados para uma nova projecção do sistema. Forrester (1971) classifica os sistemas em dois tipos de ciclos: abertos e *feedback* ou recursivos. No sistema de ciclo aberto, não há reconhecimento

e reacção à sua própria performance, além que a acção passada não controla a sua acção futura. Estes sistemas são caracterizados por relações causa e efeito lineares, sem retro alimentação. O sistema de ciclos de *feedback* ou recursivos sofrem influência pelo seu comportamento passado, onde causa e efeito se confundem, sendo a sua estrutura que determina o seu comportamento.

Goodman (1989) afirma que os ciclos de *feedback* ou recursivos podem ser representados por um conjunto de causas interligadas, que em função de estruturas e actividades geram respostas e comportamentos. Quando uma acção uma variação no mesmo sentido, origina-se um *feedback* positivo ou de reforço, quando em sentido contrário é produzido um *feedback* negativo ou de equilíbrio. Quanto à modelação de sistemas, segundo os conceitos dos Sistemas Dinâmicos, podem ser modelados por métodos qualitativos ou quantitativos.

Hoje existem diversos softwares, como o Vensim, Stella, iThink e PowerSim que podem ser utilizados em computadores pessoais para a implementação de modelos de sistemas, também chamados de "simuladores de voo" para as ciências em geral, numa analogia com os simuladores de voo tradicionais já amplamente utilizados nos computadores pessoais e que ajudam a aprender a pilotar aviões "sem utilizar aeronaves".

O MIT-MA-USA, local de trabalho do Prof. Dr. Jay W. Forrester, tem sido o grande pólo gerador de grande parte das pesquisas cientificas na aplicação do Pensamento Sistémico em todas as áreas da ciência e das principais aplicações na educação como o projecto "System Dynamics and Learner – Centered Learning in Kindergarten through 12th Grade Education", que está a ser implementado em centenas de escolas nos Estados Unidos da América. Projectos semelhantes estão a ser implementados na Dinamarca, Noruega, Suécia, Finlândia, Inglaterra, Holanda e outros países.

2.3.2. Vantagens dos Sistemas Dinâmicos

O uso de simulação em sistemas dinâmicos apresenta as seguintes vantagens:

- Combinam a teoria, métodos e filosofia para analisar o comportamento de sistemas em diversas áreas como a engenharia, saúde, gestão, etc;
- Ajudar a compreender como e porquê as alterações acontecem ao longo do tempo;
- Os primeiros artigos relativos a Sistemas Dinâmicos aparecem na Harvard Business Review (Forrester, 1958);
- São utilizados para melhor compreender os meios sociais e económicos.
- Utilizam o conceito de "campo de Controlo de Feedback" para organizar informações na forma de modelos para simulação computacional.

2.3.3. Importância dos Sistemas Dinâmicos

Os Sistemas Dinâmicos são importantes pelas seguintes razões:

- É uma metodologia utilizada para entendermos "como" os sistemas se modificam ao longo do tempo;
- É uma ferramenta que permite a criação de laboratórios de aprendizagem;
- Permite o apoio do processo de aprendizagem, permitindo conhecer melhor as organizações.
- Os sistemas apresentam padrões circulares de causa e efeito, chamados ciclos de re--alimentação ("feedback") de fácil representação;
- Mostram os relacionamentos das variáveis do sistema, sendo melhor compreendidos.

2.3.4. Software de Sistemas Dinâmicos – Vensim PLE

Vensim PLE (Personnel Learning Edition) - Vensim é uma ferramenta de modelação visual que permite desenvolver, documentar, simular e analisar modelos de sistemas dinâmicos. Criada por Ventana Systems, Inc., foi delineada para tornar mais fácil a assimilação da Dinâmica de Sistemas **(Figura 2.13)**. Este software fornece um modo simples de construir modelos de simulação a partir de diagramas causais ou de diagramas de fluxo (como os do STELLA). Há um editor de equações que auxilia a completar o modelo. Uma vez completo, poder-se-á explorar o comportamento do modelo.

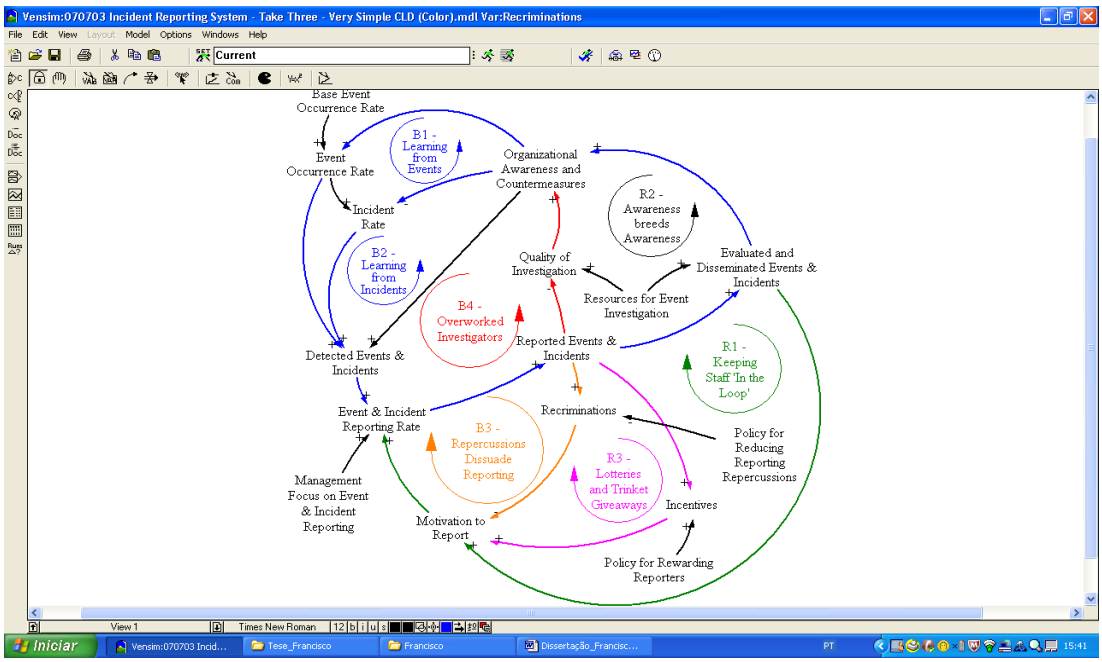


Figura 2.13 – Software de Sistemas Dinâmicos Vensim PLE

Os vários resultados simulados podem ser apresentados numa só janela permitindo a sua observação e interpretação mediante a alteração sistemática das várias variáveis, parametrizando o tipo de gráfico escolhido, assim como as variáveis a apresentar no *Output* final.

2.4. O Modelo Dinâmico de Gestão de Incidentes

2.4.1. Introdução

O conceito de gestão do conhecimento seguro tem uma dupla natureza, que surge quando se analisam os propósitos de segurança e segurança da informação nas organizações. Para este estudo, não se distingue os conceitos de conhecimento, dados, informação e sabedoria. Isso não se reflecte na importância dessa taxionomia, que foi abordada por muitos outros (Davenport, 1997; Halal, 1998; Holzapple e Joshi, 2004; O'Dell e Grayson,1998; Stewart, 1997; Sveiby, 1997). Em vez disso, é abordada especificamente uma outra questão: será que estamos a assegurar a segurança do conhecimento, da gestão da segurança da informação, ou ambos?

A primeira parte da dualidade, garantindo a segurança do conhecimento enquanto um activo, pode ser pensada como um processo em que se garante a sua correcta e adequada utilização no suporte à missão do proprietário (ISO / IEC, 2005). Ao mesmo tempo, garantir a segurança do conhecimento inclui também a prevenção do uso indevido, seja ele intencional ou não, de fontes tanto internas como externas (Haley et al., 2005). A confidencialidade da informação, a sua integridade, a sua disponibilidade e não-repudio (CIA-NR) são uma pedra angular das operações seguras, e o seu apoio tem sido a preocupação tradicional de grande parte da tecnologia de segurança da informação: criptografia, *firewalls*, detecção de intrusão, e um grande número de outras ferramentas (norma ISO / IEC, 2005; National Institute of Standards e Tecnology, 2000). A estratégia da "defesa em profundidade", onde a utilização de várias tecnologias em sobreposição são utilizadas para melhorar o perfil de segurança da empresa, tem sido fortemente recomendada há já algum tempo (National Institute of Standards and Tecnology, 2001).

A segunda parte da dualidade, a gestão da segurança do conhecimento, diz respeito à recolha, validação e aplicação de informações relacionadas à segurança em benefício da empresa. Muitas das tecnologias citadas acima protegem e relatam as suas actividades. A capacidade de usar esse conhecimento de forma a modificar e manter pró activamente um perfil de segurança forte, é crucial para um sucesso continuado em face da rápida evolução

das ameaças. Além disso, uma disseminação bem sucedida de lições aprendidas com falhas de segurança ocorridas no passado e "*quase-acidentes*" é importante para o desenvolvimento de uma consciência de segurança dentro da cultura da empresa. Esta consciência pode ajudar a prevenir futuros imprevistos e dar aos colaboradores um marco coerente de forma a estes julgarem e avaliarem suas acções.

A complexidade da gestão da informação sobre segurança aumenta rapidamente, tal como as ameaças à segurança. O aumento de volumes de ataques e a sofisticação destes tem vindo a crescer (Gordon et al., 2004). Soluções fortuitas ou unidimensionais que negligenciem estas mudanças não oferecem protecção suficiente num ambiente em mudança (Campbell, 2006); por outro lado, ferramentas adaptáveis para detecção e mitigação de ataques e anomalias estão ainda numa fase embrionária de desenvolvimento (Debar e Viinikka, 2005). Assim, a necessidade tanto de uma gestão segura do conhecimento como de uma gestão de informações de segurança deverá continuar a existir.

2.4.2. Os desafios organizacionais

Gold et al. (2001) identificam três dimensões-chave na capacidade da infra-estrutura de uma organização dar suporte a um programa de gestão tecnológica, estrutural e cultural, com questões não-técnicas muitas vezes a determinarem o resultado do programa (Damodaran e Olphert, 2000). O suporte estrutural a programas de gestão do conhecimento assume a forma de alocação de recursos de uma organização e a afirmação pública dos objectivos desses sistemas (Debowski, 2006). A capacidade de uma organização para alterar os padrões de interacção entre os seus colaboradores, processos e tecnologias para explorar os seus activos de conhecimento depende da compreensão de sua cultura organizacional (Bhatt, 2001). Essas abordagens sobre os elementos estruturais e culturais da gestão dos sistemas de conhecimento reflectem a realidade do comportamento organizacional, que é pouco racional, menos que ideal em termos económicos e conduzido, em grande parte, satisfazendo as exigências contraditórias dos múltiplos intervenientes.

Antes de uma violação de segurança ocorrer, é difícil estimar os benefícios de assegurar a segurança da informação, em relação a outros investimentos. Após uma falha de segurança, as perdas económicas, por sua vez geram dúvidas acerca de decisões anteriores (Gordon et al., 2004). Embora os modelos económicos existam para orientar as empresas nas suas decisões de alocação (Gordon e Loeb, 2002), estas nem sempre reconhecem o completo valor económico total ou estratégico da prevenção de erros (Repenning e Sterman, 2001). Um sistema para gerir a segurança do conhecimento em benefício da empresa fornece um valor preventivo semelhante, mas a sua importância percepcionada pode não ser clara na

ausência de falhas. Na verdade, o sucesso em evitar problemas e dissuasão de eventuais invasores podem criar complacência.

Além disso, as percepções individuais da importância de segurança em relação a outras pressões na empresa podem criar um preconceito contra a elaboração de relatórios incidentes. Embora a necessidade da formação dos utilizadores, em prol de uma organização segura seja muitas vezes discutido, estes podem considerar as normas de segurança fortes como intrusivas, pouco práticas, ou em desacordo com as suas contribuições para o lucro. Estudos de aceitação da tecnologia (Davis, 1989; Venkatesh e Davis, 2000) explicitamente consideram a utilidade percepcionada como um importante factor de êxito. Se a recolha e difusão de conhecimentos de segurança não forem vistos como um factor que contribui para a prossecução dos objectivos da empresa orientados para a produção, serão desvalorizados. Podemos encontrar um paralelo a isto na segurança industrial, onde fortes pressões económicas no sentido de manter a produção podem ter efeitos prejudiciais para a segurança (Cooke e Rohleder, 2006). A resistência à partilha do conhecimento também pode surgir quando as pressões competitivas internas da empresa criam resistência aos controlos de segurança adequados (Moon e Park, 2002).

Uma gestão do conhecimento seguro bem sucedida deve ter em conta os efeitos da denúncia sobre o indivíduo e a empresa, dado que os desincentivos podem ser difíceis de eliminar. No domínio das notificações de segurança, por exemplo, quando os relatórios de incidentes têm de subir na hierarquia até chegar aos decisores que hão-de actuar, os intermediários podem bloquear um relatório que indica a sua responsabilidade por negligência ou culpa (Johnson, 2003). As relações pessoais dentro da empresa podem limitar seu cumprimento. O sentido de lealdade de um colaborador para com um colega de trabalho ou um superior hierárquico podem impedi-lo de partilhar conhecimentos que podem ser prejudiciais à sua reputação ou à sua carreira (Johnson, 2003; Phimister et al., 2003). Relatórios anónimos ou confidenciais registam maiores taxas de sucesso em termos de participação (Lee e Weitzel, 2005), embora ao remover informações de identificação, detalhes importantes do problema também podem ser perdidos, reduzindo assim a eficácia do sistema.

Há também registo de um conhecimento limitado da presença de problemas de segurança ou comportamento de risco entre pessoal fora da área de segurança. Existe uma adopção generalizada de ferramentas simples de segurança como firewalls e software antivírus. Ao mesmo tempo, porém, erros comuns e "Higiene de segurança" limitada podem ser atribuídos a alguma desconexão cognitiva ou social entre as prioridades do pessoal de segurança e as prioridades daqueles que protegem, criando uma lacuna na cultura de segurança (Schneier, 2000; Winkler, 2005).

Do ponto de vista da empresa, um conjunto de falhas de segurança e eventos podem, por si só, tornar-se um importante alvo para o ataque. Tais conhecimentos sensíveis podem incluir relatórios de incidentes que demonstram a consciência de uma organização de uma situação potencialmente perigosa que, se não for corrigida, poderia levar a um acidente. Foi observado que um conhecimento antecipado de uma situação perigosa pode ter uma grande influência se os danos punitivos forem avaliados em litígio (Johnson, 2003).

Por fim, a notificação de incidentes precisa ir além dos limites tradicionais da organização. O estudo de ataques internos do USSS-CERT / CC nas instituições do sector bancário e financeiro constatou que 83% das violações nas suas bases de dados foram pela primeira vez observados por indivíduos fora da empresa-alvo, e não por pessoal interno (Randazzo al., 2004).

Nenhum destes problemas é surpreendente, e nenhum é intransponível. A implementação de sistemas que visam a gestão de informação segura requer mais do que soluções tecnologicamente sólidas. Exige fortes incentivos económicos, apoio formal e informal, uma ligação clara às necessidades do modelo de negócio, acompanhamento e execução para garantir o cumprimento (Gordon e Loeb, 2002; Haley et al., 2005; Stanton e Stam, 2006). Todos estes factores devem ter em conta como gestores, colaboradores e técnicos de informação vêem a segurança da informação através dos seus próprios olhos, e criar uma síntese das necessidades e compromissos. Esta integração dos vários aspectos organizacionais do conhecimento seguro pode tornar-se nos alicerces de uma poderosa cultura de segurança na empresa.

2.4.3. Os sistemas de notificação de incidentes de segurança como um modelo de gestão de conhecimento seguro

A base teórica surge das semelhanças entre os sistemas de notificação de segurança industriais e os sistemas de segurança. Os sistemas de notificação de segurança, são particularmente aqueles ligados às preocupações com falhas catastróficas e os seus efeitos na saúde e no ambiente, já são usados há décadas. Uma das consequências das falhas de segurança é, frequentemente, o reconhecimento tardio das falhas de informação ─ não da tecnologia de informação em si, mas dos processos humanos que limitam a codificação, disseminação ou reconhecimento de situações potencialmente perigosas através da organização. Para gerir esta informação, indústrias e governos desenvolveram múltiplos sistemas que requerem a notificação de falhas de segurança. Estes sistemas são imperfeitos e a sua eficácia é limitada pelo voluntarismo de individuais e da organização em identificar vulnerabilidades, eventos, ou riscos potenciais nas suas operações.

Os sistemas de notificação de incidentes debruçam-se sobre um tipo específico de dados sensíveis: erros, erros de avaliação e falhas nas práticas da organização que possam afectar os resultados correntes ou futuros. Um incidente significativo pode expor a empresa à perda financeira, a um possível escrutínio das entidades reguladoras e perda de reputação e quota de mercado. Mesmo aqueles eventos anómalos que não causam estragos de maior, podem ser cuidadosamente escrutinados de forma a expor falhas no processo ou conhecimento.

Tanto os sistemas de notificação de incidentes como de gestão de conhecimento seguro existem num contexto onde a tecnologia, a economia e teoria organizacional se combinam. Os utilizadores destes sistemas de notificação de incidentes enfrentam exposição de erros de curto-prazo, erros de cálculo, falhas de visão e insuficiências próprias e nos seus ambientes de trabalho, criando conflitos que afectam os incentivos à sua participação. Nos ambientes de trabalho seguros, os utilizadores são tentados a usar atalhos e a contornar as boas práticas de segurança. Um sistema de notificação poderia expor estas decisões e criar conflitos idênticos entre as práticas desejadas e o verdadeiro comportamento. Isto motiva uma análise dos sistemas de notificação de incidentes como um exemplo do que se poderia esperar aquando da criação de um sistema para a gestão do conhecimento seguro.

Apesar da longa experiência em sistemas industriais de notificação de incidentes, estes continuam a ser afectados pela falta de qualidade no relato de incidentes (Johnson, 2003). Uma observação interessante é que o mesmo tipo de problemas ocorre recorrentemente em vários tipos de indústrias. Isto indica que poderá existir uma estrutura dinâmica geral que é válida para muitas destas situações.

2.4.4. Estrutura do modelo e pressupostos

O modelo apresentado (Sveen, Rich, Jager, 2007) nas **Figura 2.14, 2.15 e 2.16** é uma síntese de muitos casos de várias indústrias diferentes. O modelo foi criado usando a abordagem de feedback de Sistemas Dinâmicos, e implementado utilizando o software Vensim (Sveen, Rich, Jager, 2007). Os Sistemas Dinâmicos encaram os sistemas como governados por feedback, informações, atrasos materiais, e acumulações. Providenciam uma compreensão de problemas complexos através de uma análise de como a estrutura de um sistema influencia o seu comportamento ao longo do tempo (Forrester, 1961; Richardson e Pugh, 1981; Sterman, 2000).

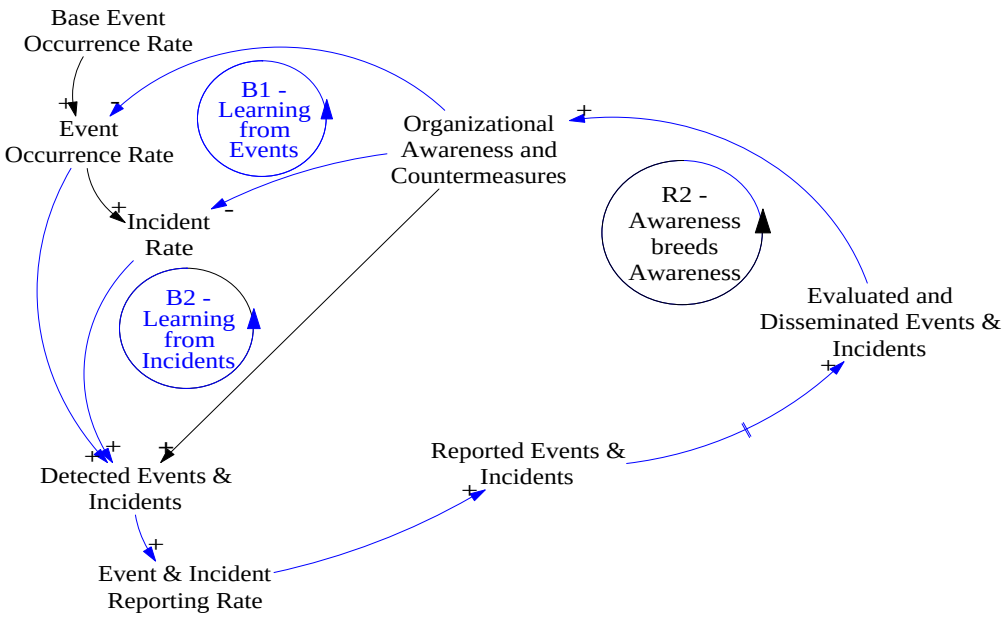


Figura 2.14 – Modelo do sistema de reporte de incidentes

(Aprendendo com os incidentes e eventos)

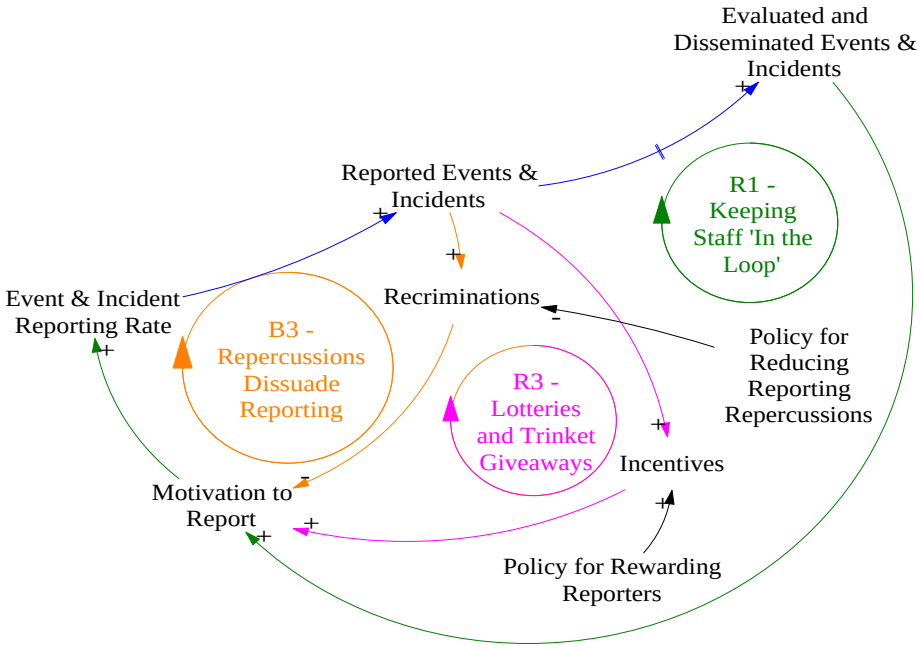


Figura 2.15 – Modelo do sistema de reporte de incidentes

(Incentivos, recriminações e *feed-back* da equipa)

A estrutura do modelo inclui ciclos casuais que descrevem como os eventos e incidentes são notificados e utilizados para a aprendizagem organizacional. É de notar a distinção entre incidentes e eventos. Aqui, um evento é definido como uma situação imprevista ou "quase-acidente", gerido por um custo muito baixo ou nulo no curto prazo. Se um evento não é remediado, torna-se num incidente que tem um custo imediato ou consequência, como um dano. Os eventos são reduzidos de acordo com uma curva de experiência segundo a lei de potência: cada vez que a quantidade de incidentes apropriadamente investigados duplica, a taxa de ocorrência de incidentes e eventos é reduzida numa certa percentagem, reflectindo uma aprendizagem gradual a partir da experiência sobre incidentes e eventos.

O modelo apresentado aqui não trata de como os incidentes são criados. Ao invés, o modelo tenta explicar como a aprendizagem pode ocorrer a partir da notificação de incidentes e eventos, de forma a prevenir futuros incidentes. A origem dos incidentes é, portanto, exterior ao modelo e é mantida constante, '*Base Event Occurence Rate*" (**Figura 2.14**). Esta constante representa o que o número de eventos e, portanto, o potencial para a ocorrência de incidentes teria sido sem nenhumas contra medidas ou consciência organizacional.

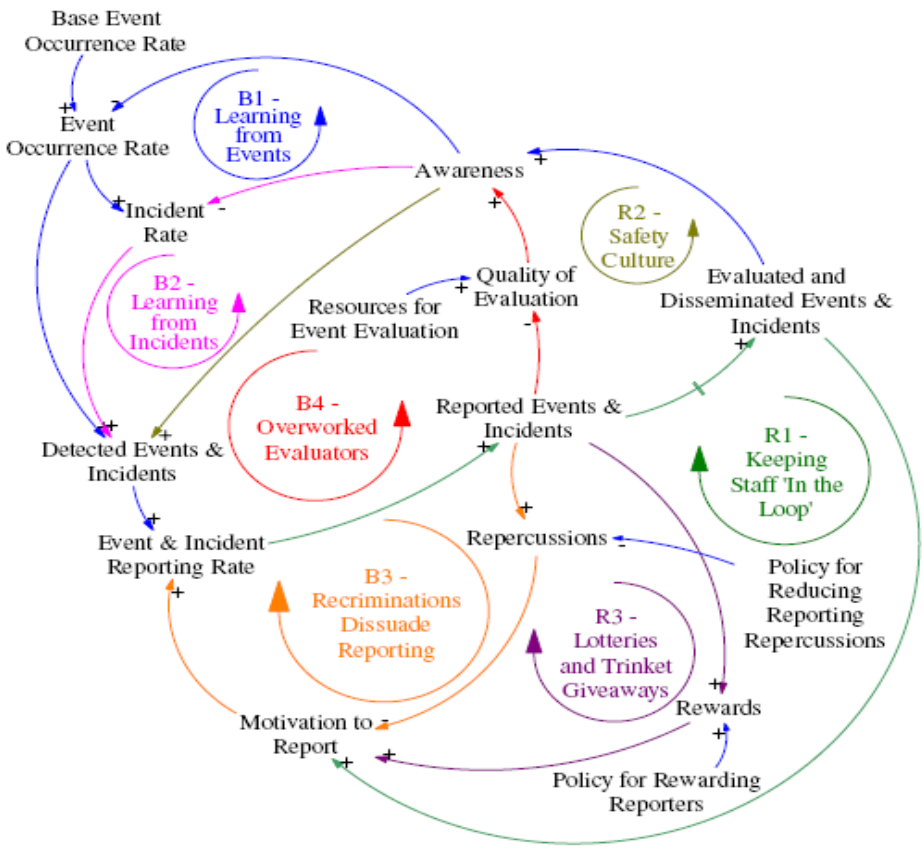


Figura 2.16 – Visão Global do Modelo do sistema de reporte de incidentes

2.4.5. Aprendendo com os incidentes e eventos

Geralmente, o objectivo de um sistema de notificação de eventos é partilhar informação sobre incidentes, de forma a evitar a sua recorrência ou minimizar os danos. Quando um incidente ocorre, alguém tipicamente como um operador, uma enfermeira ou um piloto, detecta-o e faz a respectiva notificação. Num ambiente de gestão de incidentes ideal, uma equipa de investigação entraria então em campo, numa tentativa de descobrir a origem sistémica desse incidente. Se tiver sucesso, medidas podem ser tomadas e o pessoal passará a ter conhecimento não só do perigo, mas igualmente do problema que o causou. Estas medidas ajudam a evitar futuras ocorrências do mesmo incidente ou, no caso de um evento, prevenir a sua transformação num incidente. À medida que o pessoal ganha sensibilidade nas questões de segurança, tornam-se mais eficazes a detectar incidentes potenciais e a quantidade de eventos e incidentes reportados aumenta (**Figura. 2.14, ciclo R2**). Na linguagem de Sistemas Dinâmicos, *B1-Learning from Events* e *B2- Learning from Incidents* são ciclos de feedback em equilíbrio, onde uma pressão exógena irá gerar ajustamentos endógenos de forma a compensar a pressão no sistema. Neste caso, os ciclos *B1-Learning from Events* e *B2- Learning from Incidents* descrevem um aumento na ocorrência de novos eventos aumentando o conhecimento, o que incrementa o grau de prontidão e reduz a ocorrência de eventos no futuro. *R2 – Awareness breeds Awareness,* descreve como uma capacidade de detecção melhorada aumentando a consciência da segurança, o que cria pressões endógenas que ainda a reforçam mais; a isto chama-se um ciclo de feedback de reforço. Os ciclos de feedback em equilíbrio poderosos, que contrariam o efeito de *R2 – Awareness breeds Awareness,* serão descritos posteriormente.

2.4.6. Motivações para notificar

À medida que a equipa se apercebe que as notificações feitas aumentam a segurança da organização, a sua motivação para notificar também aumenta (**Figura 2.15, R1**). De igual modo, se a sua percepção for de que as suas notificações não levam a melhorias, a equipa pode-se sentir desencorajada a continuar. Johnson chamou a isto manter a equipa "em ciclo" (Johnson, 2003). A questão pode não ser só de feedback da equipa, mas igualmente de feedback das organizações. Um exemplo é o uso, em Taiwan, de elaboração obrigatória de relatórios relativos a incidentes de aviação à administração de aviação civil de Taiwan (CAA). Lee e Weitzel (2005) revelaram que a base de dados de incidentes de aviação da CAA contém uma quantidade considerável de dados de incidentes, mas devido a problemas de financiamento, esses dados não foram usados em análise de tendências. Além disso, os dados foram tornados inacessíveis e, portanto, não foram usados pelas transportadoras aéreas

de Taiwan, ou pelo Conselho de Segurança Aérea de Taiwan (um grupo de investigação de incidentes de aviação de Taiwan). Se aceder aos dados for difícil, os benefícios da notificação parecerão limitados aos potenciais utilizadores.

Muitas organizações utilizam incentivos para aumentar o grau de notificação. Neste modelo, os incentivos são aqueles que têm um efeito positivo na notificação. Se um incentivo tem um efeito perverso, como por exemplo, se for um dissuasor da notificação, é considerado como não tendo efeito de todo, ou como uma recriminação. Outro factor importante na motivação à notificação são as repercussões negativas que existem dentro e fora das organizações. Acções punitivas da gestão, colegas de trabalho que vejam aquele que notifica como sendo desleal, exposição aos *media*, acções legais e cultura são alguns dos factores que podem dissuadir a notificação (Anderson e Webster, 2001; Johnson, 2003; Lee e Weitzel, 2005; Phimister *et al.*, 2003).

2.4.7. Investigação de incidentes e de eventos

A última parte do modelo diz respeito à qualidade das investigações. Se a qualidade for muito baixa, como por exemplo quando a origem sistémica dos incidentes não for encontrada, o grau de percepção da organização não aumentará e eventuais salvaguardas que sejam postas em curso não serão eficientes. Nas palavras de Johnson, "os sistemas de notificação de incidentes podem proporcionar avisos importantes sobre os perigos potenciais. Todavia, em casos extremos estes avisos podem parecer-se mais com ladainhas repetitivas de procedimentos de treino do que recomendações pró-activas de segurança. Ao longo do tempo, a repetição continuada destes avisos dos sistemas de notificação de incidentes é um sintoma de problemas mais profundos nos sistemas que os utilizadores têm de usar" (Johnson, 2003).

Vários pressupostos simplificadores podem ser aplicados nesta altura. No modelo, a qualidade da avaliação é simplificada como uma função da quantidade de recursos disponíveis e carga de trabalho. Na realidade, o nível de treino e grau de experiência do investigador também têm uma palavra a dizer. Todos os eventos e incidentes têm o mesmo grau de severidade; no mundo real, a investigação provavelmente receberia recursos adicionais, caso incidentes sérios ocorressem. Todavia, como o modelo trabalha com médias ao longo do tempo, mais do que com eventos discretos, esta é uma simplificação razoável.

2.4.8. Validação do modelo

O modelo apresentado é exploratório, expandindo um modelo dinâmico de sistemas de notificação de segurança para a área da informática. Não nos podemos fiar nos processos

estatísticos que levam ao suporte de validação de sistemas complexos (Forrester e Senge, 1981). Os pressupostos tácitos das relações lineares e funções bem comportadas não se aplicam aos sistemas sociais onde atrasos na informação e de feedback criam comportamentos não lineares fora do âmbito da inferência estatística.

Cada um dos ciclos e das ligações no modelo representa uma declaração de efeitos possíveis, justificada por ligações à literatura, um primeiro nível de validação. O modelo representa o 'modelo mental', formado por uma pesquisa extensiva e por intuição. A importância relativa dos ciclos de *feedback* apenas pode ser examinada através de uma análise ao longo do tempo, através da simulação dinâmica. Quando as técnicas de modelação permitem uma acumulação dos efeitos ao longo do tempo, emergem interacções não lineares que mudam o comportamento aparente do sistema. Os indivíduos são notoriamente incapazes de compreender todas as consequências dos seus modelos (Forrester, 1994); podem não ser imparciais quando confrontados com a incerteza (Kahnman e Tversky, 2000), e são incapazes de processar muitas ideias simultaneamente (Kahnman, 1973). A modelação e a simulação criam imperfeições que podem ser usadas para documentar ideias, estimular o debate e criar agendas de pesquisa. A abordagem pragmática no sentido da validação de modelos complexos consiste em tentar desmontá-los e reflectir nos resultados obtidos. De cada vez que um modelo passa uma tentativa concertada de desafiar o seu conteúdo, esse sucesso aumenta a confiança nas suas conclusões (Barlas, 1989, 1996; Forrester e Senge, 1980). Em traços largos, considera-se três categorias de testes:

- ***Limites do modelo e formulação*** - O modelo é construído de forma a representar os efeitos dos eventos de segurança no interior da organização. Contém um conjunto de forças plausíveis que afectariam as tendências gerais dos indivíduos na empresa. Tornado claro estes pressupostos de tendências e foi efectuado o teste verificando se os resultados do modelo mudam quando os pressupostos variam.

- ***Validade estrutural*** - A seguir considera-se se o modelo está construído de acordo com a teoria. O modelo é consistente com as declarações descritivas sobre incentivos e desincentivos à notificação de eventos ao nível organizacional fornecidos pela literatura de notificação de segurança. Também foram efectuados testes de unidades, uma forma de análise dimensional que é capaz de detectar inconsistências matemáticas na formulação das equações.

- ***Validade comportamental*** - Outra fonte de apoio surge da revisão dos resultados da simulação dinâmica à luz de uma série de pressupostos. Para este modelo, faltaram dados reais de definições de segurança, dado que esta informação raramente é partilhada fora das organizações. Ao invés, examinou-se o comportamento do modelo em condições variadas e medimos os seus resultados. Por exemplo, examinámos o modelo em condições de equilíbrio e em condições extremas, ambos artificiais, de forma a procurar falhas de especificações escondidas.

Todavia, a falta de dados da indústria torna a validade externa do modelo limitada. O objectivo é demonstrar uma estrutura plausível que gera um comportamento em particular; neste caso, identificando a forma como os gestores podem interpretar mal a informação sobre a segurança das suas organizações ao focar mais a atenção na quantidade de notificações efectuadas do que no conteúdo e lições das mesmas. O objectivo não é fazer previsões sobre resultados numéricos, dado que a existência de demasiada incerteza nos mecanismos subjacentes tornaria esse mesmo objectivo inválido (Sveen, Rich, Jager, 2007).

3. O PROCESSO DE GESTÃO DE INCIDENTES

3.1. Introdução

Neste capítulo é analisado um processo de gestão de incidentes implementado numa empresa financeira em Portugal.

A gestão de incidentes tem por objectivo a reposição do serviço no mais curto espaço de tempo e com o mínimo impacto para o negócio, garantindo que os melhores níveis possíveis de qualidade são assegurados, assim como processo agregador de conhecimento, como um processo continuo de aprendizagem para evitar que os mesmos incidentes possam condicionar novamente o serviço prestado pela organização.

A **Figura 3.1**, apresenta a visão macro das actividades que servem de *input* e *output* à gestão de incidentes.

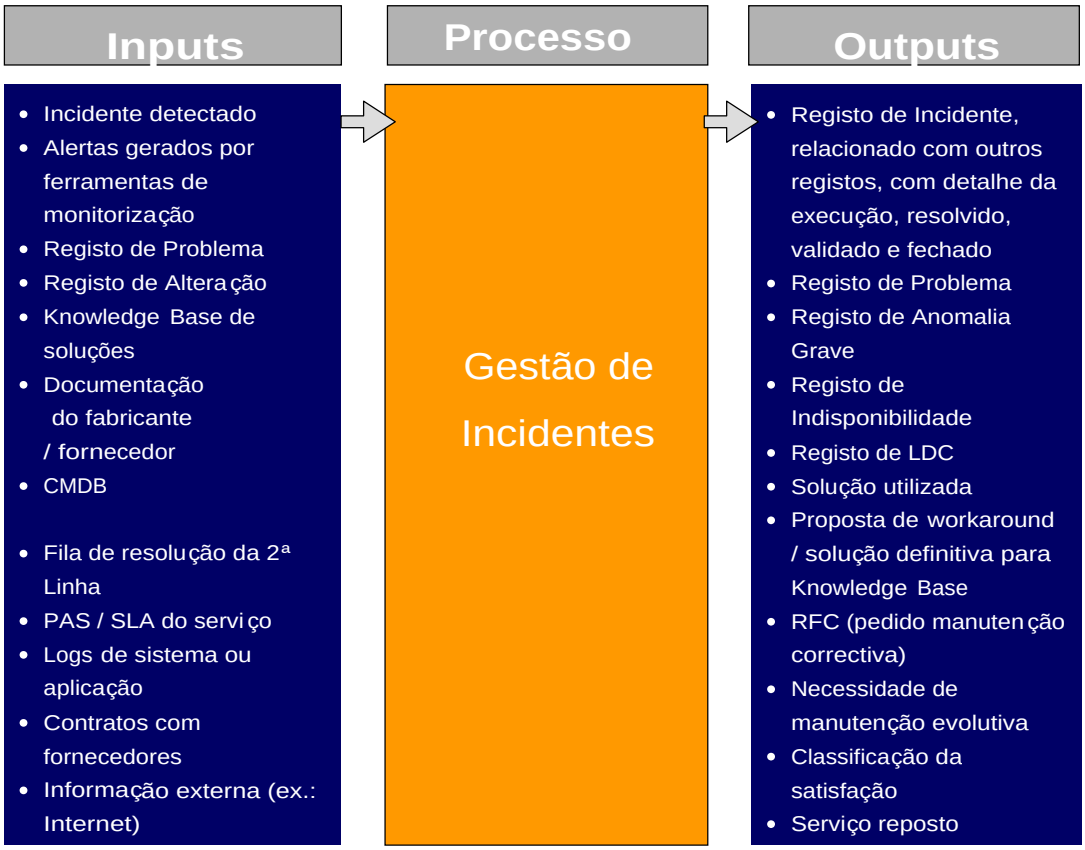
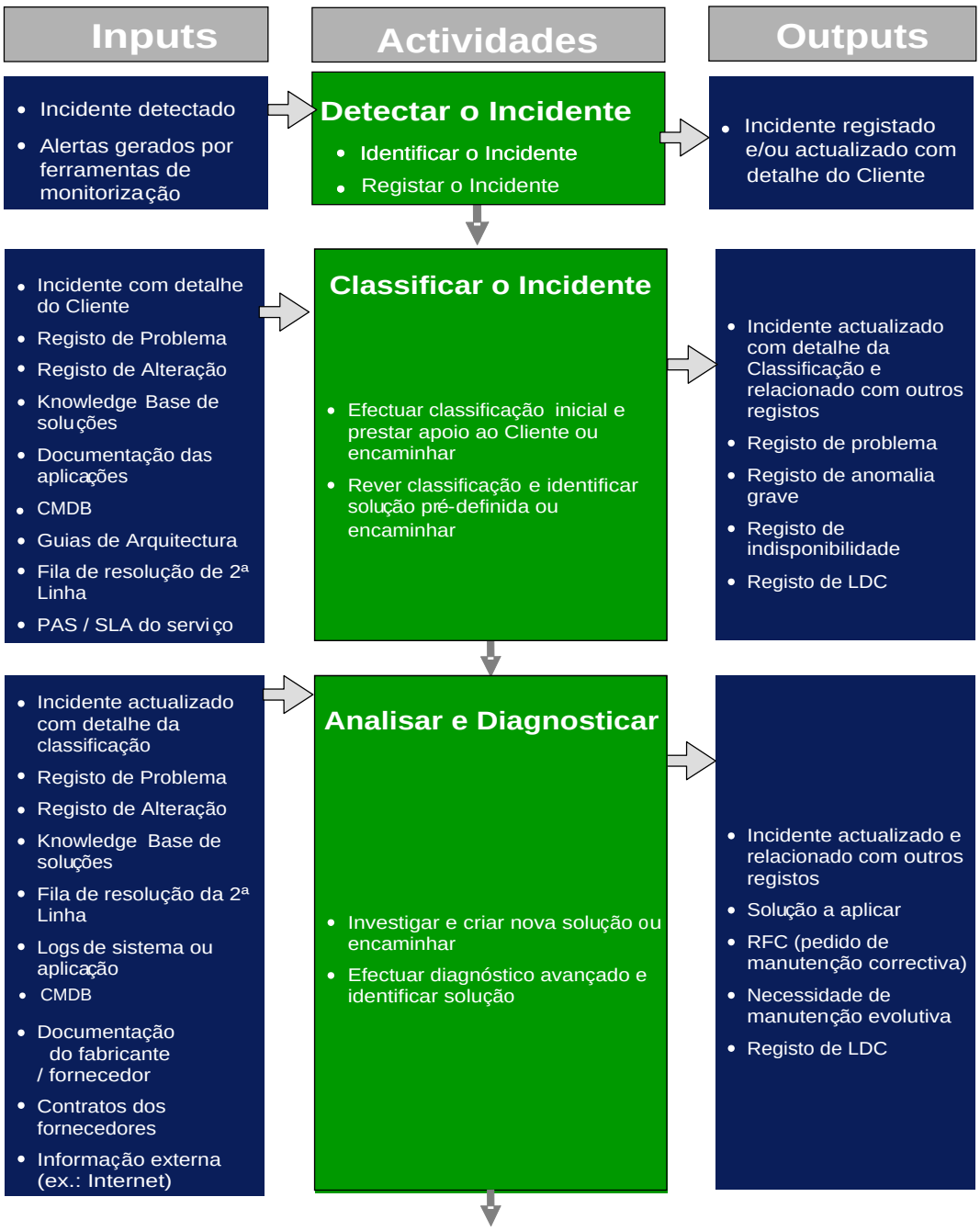


Figura 3.1 – Actividades de Input / Output do processo

Na **Figura 3.2** detalham-se as actividades internas na Gestão de Incidentes. Numa análise pormenorizada, verifica-se que este processo encontra-se implementado segundo as normas e

boas práticas correntes, existindo uma preocupação pela detecção e classificação dos incidentes, pois a partir deste momento existe um acompanhamento constante com o objectivo final de uma solução, assim como o registo numa base de dados de conhecimento de todas as intervenções com vista à sua resolução, contribuindo assim para uma prevenção de recorrências dos mesmos incidentes.



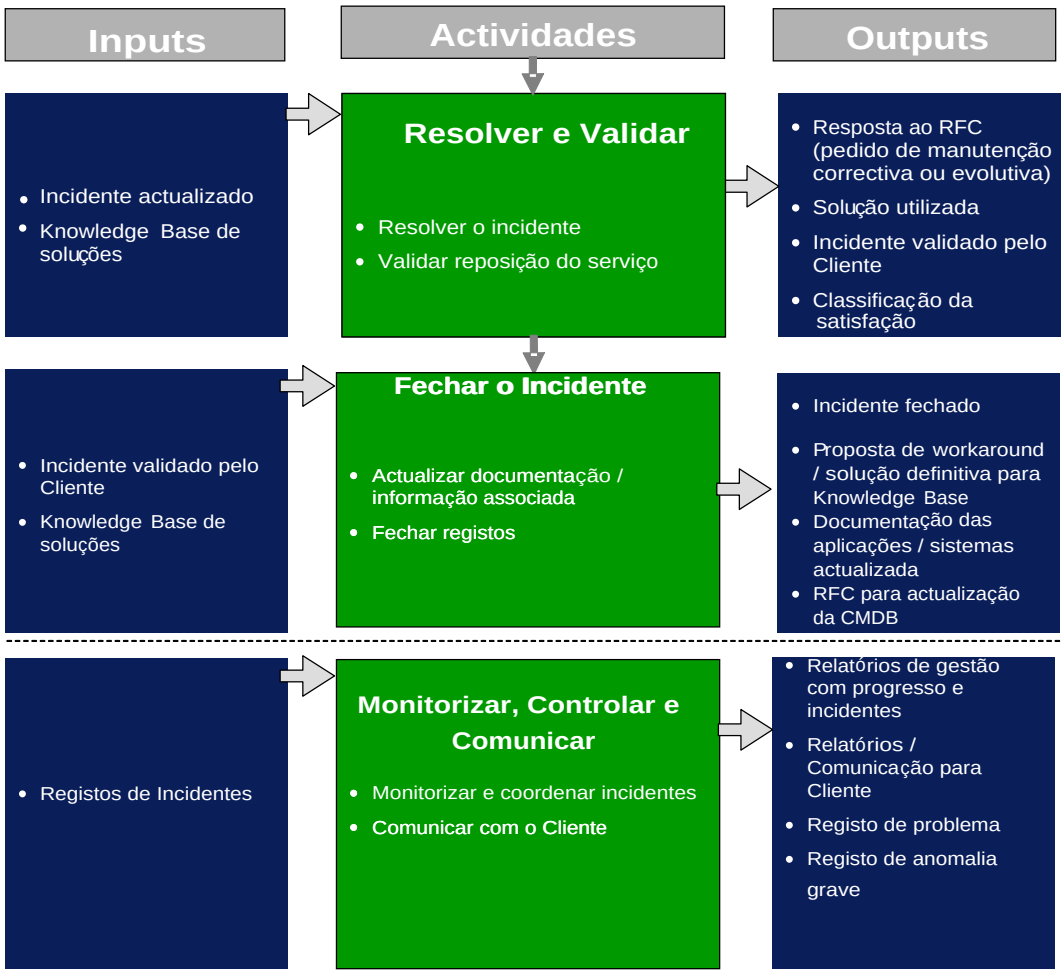


Figura 3.2 - Actividades Internas do Processo

Na **Figura 3.3** apresenta uma visão geral das relações entre as várias actividades.

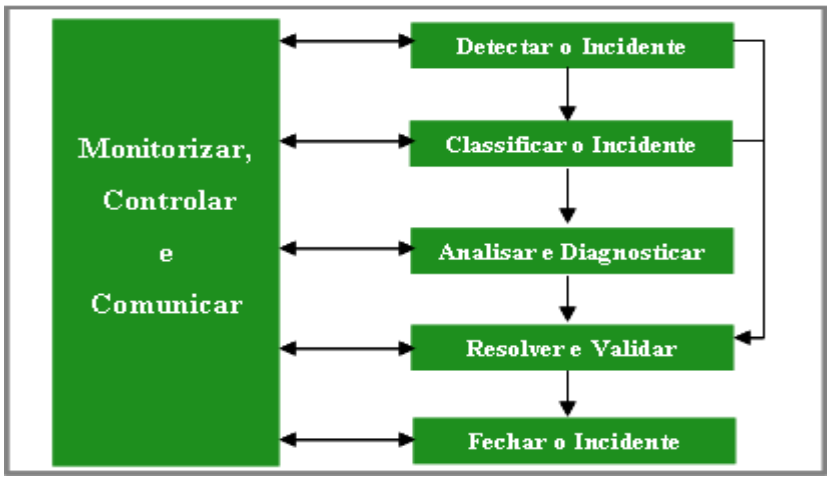


Figura 3.3 - Relação entre as actividades

3.2. Papéis e Responsabilidades

A tabela seguinte apresenta os papéis e as responsabilidades dos intervenientes na Gestão de Incidentes. Este detalhe é importante pois define em detalhe o papel e responsabilidades de cada interveniente no fluxo do processo de gestão de incidentes.

Papel	Responsabilidades	
Cliente	Qualquer pessoa que utilize os serviços disponibilizados e que detecte alguma falha no seu funcionamento.	
	Responsabilidades	• Utilizar um dos canais à disposição para reportar o incidente detectado. • Validar se o serviço voltou ao normal. • Classificar a sua satisfação com a resolução do incidente.
1ª Linha	Elemento responsável por garantir primeiro contacto com o Cliente, podendo ser, consoante a tipologia dos incidentes fornecedores externos.	
	Responsabilidades	• Registar todos os incidentes que lhe são comunicados pelo Cliente ou detectados pelos próprios. • Recolher junto do Cliente toda a informação relevante sobre o incidente e de acordo com a tipificação definida. • Efectuar classificação inicial e relacionar o incidente com outros registos (problemas, alterações, etc.), sempre que existam. • Dar apoio inicial ao Cliente. • Identificar, se existir, solução na *Knowledge Base* aplicável à 1ª Linha, caso contrário, encaminhar para a 2ª Linha. • Alertar Gestor de Incidentes de potencial problema e/ou anomalia grave. • Repor o serviço, usando a solução encontrada. • Registar utilização da solução. • Validar tecnicamente ou com o Cliente a reposição do serviço. • Actualizar documentação / informação associada ao incidente. • Fechar o incidente e outros registos associados, se existirem.

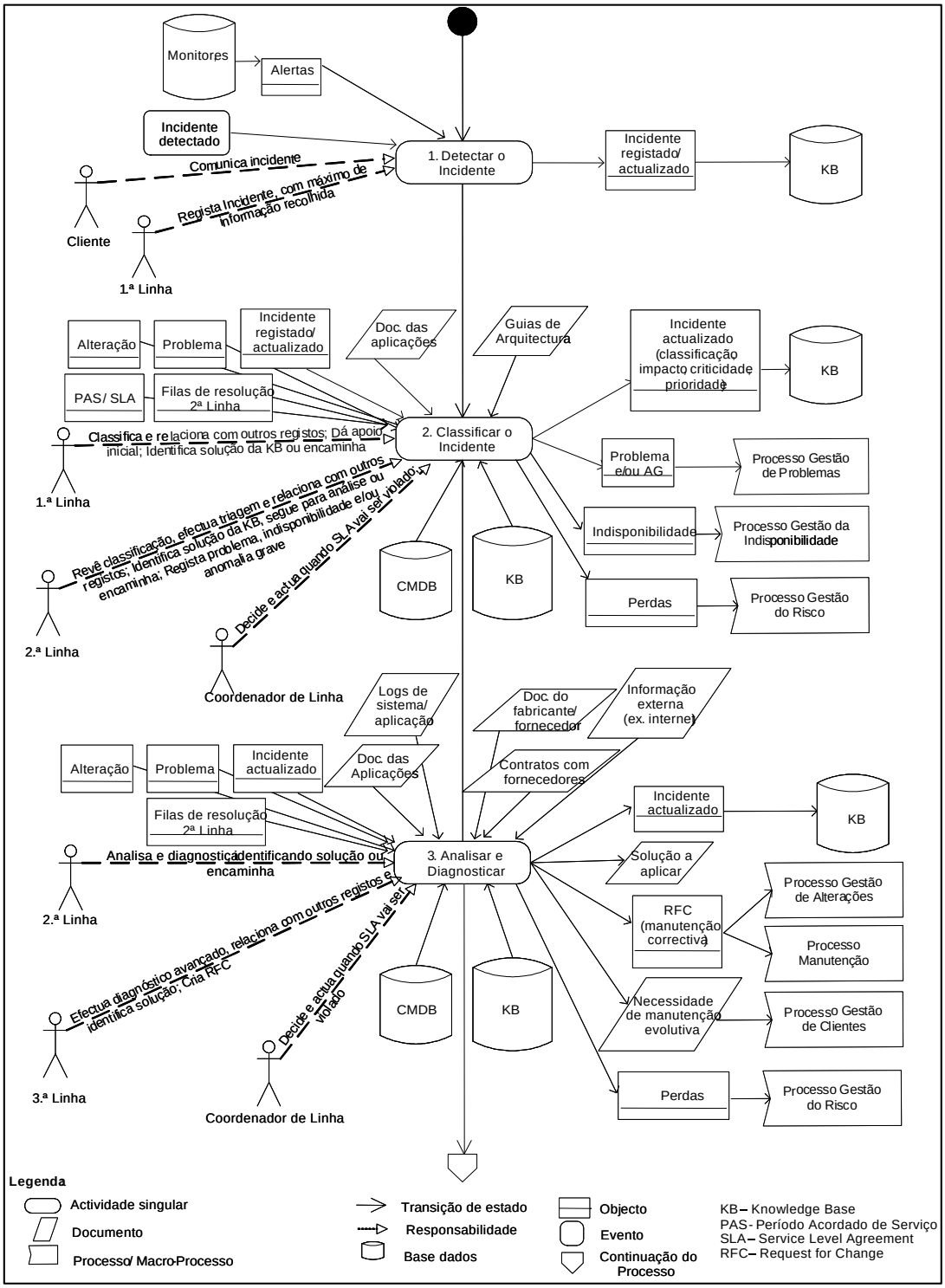
Papel	Responsabilidades	
2ª Linha	Elemento responsável por efectuar triagem mais fina e primeira análise e diagnóstico, possuindo competências técnicas gerais.	
	Responsabilidades	• Rever classificação, efectuar triagem do incidente e relacionar o incidente com outros registos, sempre que existam. • Identificar solução por procedimento predefinido na *Knowledge Base.* • Analisar e diagnosticar, identificando o *workaround* ou solução definitiva a aplicar, dentro das suas competências. • Caso não consiga efectuar nenhuma das duas anteriores, encaminhar para a 3ª Linha. • Registar problema, se for a sua equipa a resolver, ou alertar o Gestor de Incidentes para efectuar o respectivo registo. • Registar indisponibilidade, se for o caso. • Registar anomalia grave, se for o caso. • Repor o serviço, usando a solução encontrada • Registar utilização da solução. • Validar tecnicamente a reposição do serviço. • Actualizar documentação / informação associada ao incidente. • Propor registo na *Knowledge Base* da solução utilizada.
3ª Linha	Elemento responsável por resolver o incidente, caso nenhuma das outras Linhas não o tenha conseguido, sendo especialista no sistema, aplicação, plataforma, etc. onde se verifica o incidente.	
	Responsabilidades	• Efectuar o diagnóstico avançado, relacionando o incidente com outros registos, sempre que existam, e identificando o *workaround* ou solução definitiva a aplicar. • Criar RFC (Pedido de manutenção correctiva), se aplicável. • Repor o serviço, usando a solução encontrada. • Registar utilização da solução. • Validar tecnicamente a reposição do serviço. • Actualizar documentação / informação associada ao incidente. • Propor soluções para a *Knowledge Base.*

Papel	Responsabilidades	
Coordenador de Linha	Elementos responsáveis por coordenar a respectiva Linha.	
	Responsabilidades	• Decidir sobre a forma de actuar quando o SLA da Linha está prestes a ser ultrapassado. • Actuar em conformidade (assignar incidente a outro recurso, escalar hierarquicamente, etc.)
Gestor de Incidentes	Elemento responsável pela coordenação global dos incidentes e pelo bom funcionamento do processo.	
	Responsabilidades	• Controlar / coordenar casos graves, de grande volume, situações em que não se conhece o correcto encaminhamento para 2ª ou 3ª Linhas e/ou haja necessidade de envolvimento de várias equipas de 2ª ou 3ª Linhas, sem que nenhuma delas assuma a responsabilidade sobre a resolução do incidente. • Monitorizar e reportar os incidentes abertos. • Escalar hierarquicamente, quando necessário. • Registar problemas e anomalias graves, quando são detectados pela 1ª Linha ou que o próprio identifique sem que haja já registo criado.

Tabela 3.1 - Papéis e Responsabilidades

3.3. Fluxos de actividades

A **Figura 3.4**, detalha os fluxos e actividades em modo gráfico entre os vários intervenientes, mostrando como se relacionam entre si.



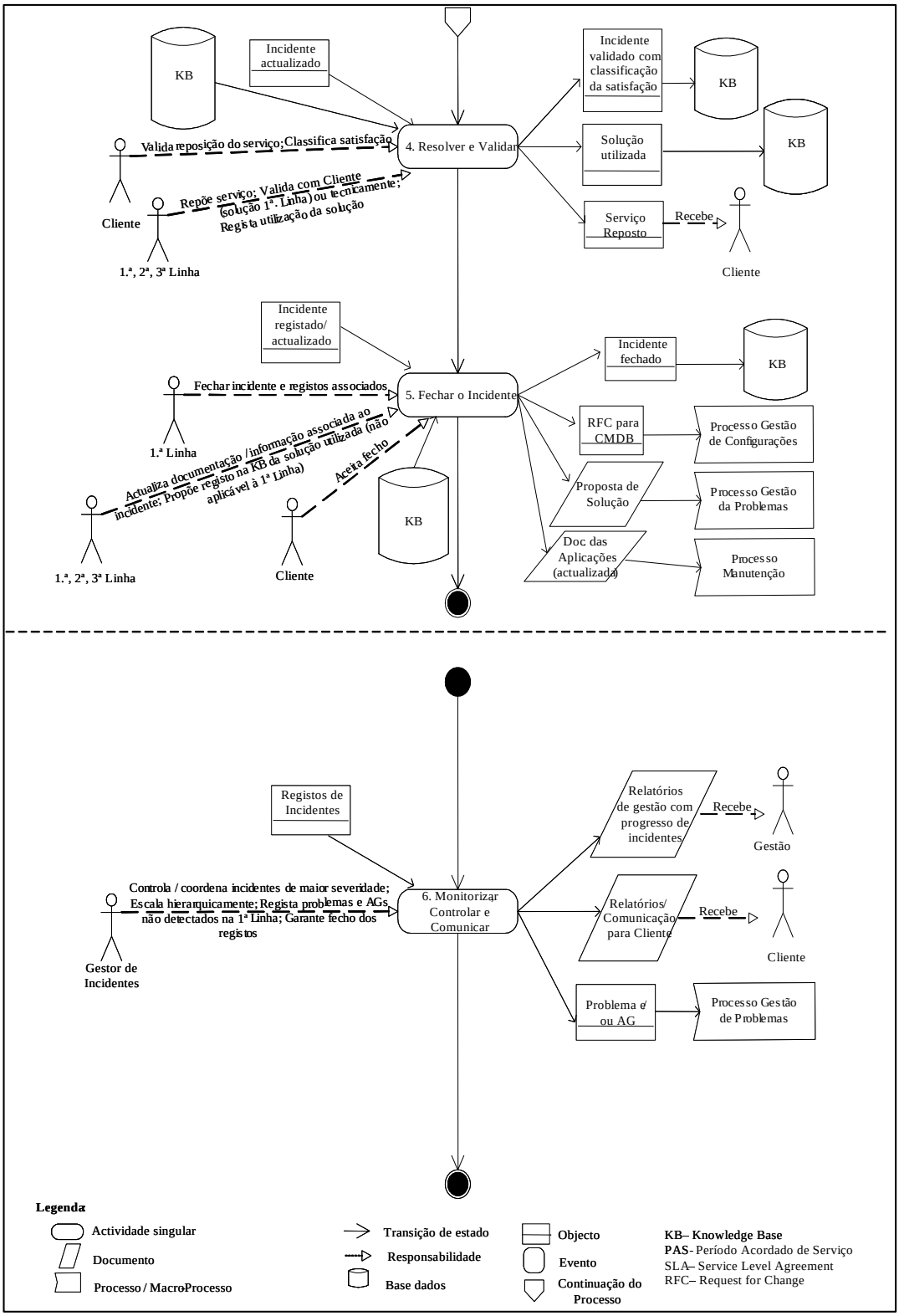


Figura 3.4 - Relação dos papéis, responsabilidades, actividades, inputs e outputs

3.4. Actividades do Processo

A Gestão de Incidentes encontra-se estruturada em 6 actividades específicas:

- **3.4.1. Detectar o Incidente**
- **3.4.2. Classificar o Incidente**
- **3.4.3. Analisar e Diagnosticar**
- **3.4.4. Resolver e Validar**
- **3.4.5. Fechar o Incidente**
- **3.4.6. Monitorizar, Controlar e Comunicar**

Descreve-se, em seguida, cada uma das actividades do Processo, com os seus objectivos, papeis e responsabilidades, tarefas, *inputs*, *outputs*, assim como as ferramentas que lhe dão suporte.

3.4.1. Detectar o Incidente

Actividade	Detectar o Incidente
Objectivos	Garantir o registo de todos os incidentes de forma tempestiva, correcta e completa, com o máximo de informação disponível.
Papéis e Responsabilidades	• Cliente – Utilizar um dos canais à disposição para reportar o incidente detectado. • 1ª Linha – Registar todos os incidentes que lhe são comunicados pelo Cliente ou detectados pelos próprios; Recolher junto do Cliente toda a informação relevante sobre o incidente e de acordo com a tipificação definida.
Inputs	• Incidente detectado (pelo Cliente ou por ferramenta de monitorização) • Alertas gerados por ferramentas de monitorização
Outputs	• Incidente registado e/ou actualizado com detalhe fornecido pelo Cliente

Tarefas	Identificar o Incidente O Cliente, perante uma situação de interrupção ou degradação de qualidade de um serviço deve comunicá-lo através de um dos canais de entrada às 1ªs Linhas, nomeadamente *Helpdesk* ou Atendimento telefónico. Alguns incidentes são detectados de forma automática pelas ferramentas de monitorização que existam.
	Registar o Incidente Nos casos em que o registo do incidente não é automático (como são os casos das ferramentas de monitorização e do *Helpdesk*), é necessário que a 1ª Linha proceda ao respectivo registo com o máximo de informação que conseguir recolher junto do cliente (atinge um ou mais utilizadores, grau de criticidade, código do erro, operação, etc.), devendo ter em conta a tipificação da informação a recolher definida de acordo com o tipo de incidente. Se a 1ª Linha verificar que o incidente já se encontra resolvido passa para a actividade "Fechar o Incidente".
Ferramentas de Suporte	
• *Helpdesk* • Atendimento telefónico • *Knowledge Data Base* • Ferramentas de monitorização existentes.	

3.4.2. Classificar o Incidente

Actividade	Classificar o Incidente
Objectivos	Classificar e prioritizar os incidentes com o máximo rigor, identificando a solução mais apropriada ou a equipa de 2ª Linha mais indicada.

Papéis e Responsabilidades	• 1ª Linha – Efectuar classificação inicial, e relacionar o incidente com outros registos (problemas, alterações, etc.), sempre que existam; Dar apoio inicial ao Cliente; Identificar, se existir, e aplicar solução da *Knowledge Base*, sempre que lhe seja possível a sua aplicação, caso contrário, encaminhar para 2ª Linha; Informar Cliente; Alertar o Gestor de Incidentes de potencial problema e/ou anomalia grave. • 2ª Linha – Rever classificação, efectuar triagem do incidente e relacionar o incidente com outros registos, sempre que existam; Identificar solução por procedimento predefinido na *Knowledge Base* ou avançar para análise e diagnóstico ou encaminhar para 3ª Linha; Registar problema, se for a sua equipa que o irá resolver, ou alertar o Gestor de Incidentes para efectuar o respectivo registo, se for o caso; Registar indisponibilidade, se for o caso; Registar anomalia grave, se for o caso. • Coordenador de Linha – Decidir sobre forma de actuar quando o SLA está prestes a ser ultrapassado; Actuar em conformidade (assignar incidente a outro recurso, escalar hierarquicamente, etc.).
Inputs	• Incidente registado e/ou actualizado com detalhe fornecido pelo Cliente. • Registo de Problema. • Registo de Alteração. • *Knowledge Base* de soluções. • Documentação das aplicações. • CMDB. • Guias de Arquitectura. • Fila de resolução da 2ª Linha (quantidade de incidentes semelhantes ou na mesma plataforma/aplicação). • PAS / SLA do serviço.
Outputs	• Incidente actualizado com detalhe (classificação, impacto, severidade, criticidade, urgência, prioridade)

	• Registo de Problema (se aplicável). • Registo de Anomalia Grave (se aplicável). • Registo de Indisponibilidade (se aplicável).
Tarefas	<u>Efectuar classificação inicial e prestar apoio ao Cliente ou encaminhar</u> A 1ª Linha, se dispuser de informação para tal, deve avaliar o domínio de impacto, a severidade e a criticidade do incidente e classificar com o máximo rigor o incidente, incluindo urgência e prioridade. Caso se comprove haver relação causa-efeito entre a implementação de uma alteração e o incidente reportado, deverá proceder-se ao relacionamento dos respectivos registos. Se dessa classificação encontrar na *Knowledge Base* uma solução aplicável em 1ª Linha (*workaround* ou solução definitiva), deverá executá-la de imediato, comunicando com o cliente para obter desde logo a respectiva validação (passa para a actividade "Fechar o Incidente"). Caso não haja solução disponível para 1ª Linha, o incidente será escalado funcionalmente para a 2ª Linha de acordo com a classificação atribuída. Nesta situação, se se verificar que já existe um problema registado, deverá ser feito o relacionamento dos registos. Caso o SLA da 1ª Linha esteja prestes a ser atingido, deverá ser notificado o Coordenador da Linha para que actue em conformidade. Caso identifique registos semelhantes, deve informar o Gestor de Incidentes sobre potencial problema, para que este possa efectuar o registo. Caso verifique que o incidente representa um impacto financeiro e/ou reputacional considerável e de consequências que extravasem o âmbito, deve informar o Gestor de Incidentes sobre potencial anomalia grave para que este possa efectuar o registo.
	<u>Rever classificação e identificar solução predefinida ou encaminhar</u> Na 2ª Linha, deve ser recolhida mais informação, analisando a sua própria fila de resolução, documentação, CMDB, etc., para ser afinada a análise de impacto e criticidade, podendo ser revista a classificação inicialmente atribuída, e efectuar um diagnóstico inicial para

	confirmação. Caso se comprove haver relação causa-efeito entre a implementação de uma alteração e o incidente reportado, deverá proceder-se ao relacionamento dos respectivos registos. Se desse diagnóstico inicial, se verificar a existência de solução aplicável à 2ª Linha na *Knowledge Base*, deverá utilizá-la, passando para a actividade "Fechar o Incidente". Caso contrário, se estiver dentro das suas competências técnicas, passará à actividade seguinte, senão, deverá escalar o incidente para a 3ª Linha, de acordo com a sua classificação e triagem inicial. Em qualquer dos casos, se verificar que já existe um problema registado, deverá ser feito o relacionamento dos registos. Caso o SLA da 2ª Linha esteja prestes a ser atingido, deverá ser notificado o Coordenador da Linha para que actue em conformidade. Caso identifique a existência de um problema, deverá registá-lo e relacioná-lo com o incidente, caso a resolução fique a cargo da sua equipa, senão, deverá alertar o Gestor de Incidentes para que este efectue o registo. Caso identifique que o impacto do incidente em termos financeiros e/ou reputacionais é considerável e as suas consequências extravasam o âmbito, deve efectuar o registo de uma anomalia grave e relacioná-lo com os incidentes. Caso identifique que o incidente é crítico, deve avisar o Coordenador do Comité de Crise. Caso identifique que o serviço se encontra indisponível, deverá criar também o registo de indisponibilidade e relacioná-lo com o incidente. Se se tratar de uma indisponibilidade planeada, o respectivo registo de indisponibilidade deverá ser relacionado com o do incidente.
Ferramentas de Suporte	
• *Knowledge Data Base* (Gestão de Incidentes, Gestão de Problemas, Gestão de Indisponibilidades, Gestão de Configurações)	

3.4.3. Analisar e Diagnosticar

Actividade	Analisar e Diagnosticar
Objectivos	Analisar e diagnosticar o incidente no sentido de encontrar uma solução para restabelecer o serviço, caso não haja soluções conhecidas na *Knowledge Base* para resolver o incidente.
Papéis e Responsabilidades	• 2ª Linha – Analisar e diagnosticar, identificando o *workaround* ou solução definitiva a aplicar, dentro das suas competência ou encaminhar para 3ª Linha. • 3ª Linha - Efectuar o diagnóstico avançado, relacionando o incidente com outros registos, sempre que existam, e identificando o *workaround* ou solução definitiva a aplicar; Criar RFC (pedido de manutenção correctiva), se aplicável. • Coordenador de Linha – Decidir sobre forma de actuar quando o SLA está prestes a ser ultrapassado; Actuar em conformidade (assignar incidente a outro recurso, escalar hierarquicamente, etc.).
Inputs	• Incidente actualizado com detalhe (classificação, impacto, urgência, prioridade, *activity log*). • Registo de Problema. • Registo de Alteração. • *Knowledge Data Base* de soluções. • Fila de resolução da 2ª Linha (quantidade de incidentes semelhantes ou na mesma plataforma/aplicação). • *Logs* de sistema ou aplicação. • CMDB. • Documentação da Aplicação. • Documentação do fabricante / fornecedor. • Contratos com fornecedores. • Pesquisa externa (ex.: Internet).
Outputs	• Incidente actualizado com detalhe (*activity log*) • Solução a aplicar

	• RFC (Pedido de manutenção correctiva) (se aplicável). • Necessidade de manutenção evolutiva (se aplicável).
Tarefas	<u>Investigar e criar nova solução ou encaminhar</u> A 2ª Linha, em algumas situações, dentro das suas competências, deve investigar *logs*, documentação, internet, etc. para determinar uma nova solução para o incidente, passando à actividade seguinte. Caso a nova solução origine a criação de um RFC (Pedido de manutenção correctiva). Nestas situações, o Cliente deve ser informado do tempo de execução da solução, mantendo-se o incidente em aberto até ser concluída a alteração. Caso se identifique que a solução passará por uma manutenção evolutiva deverá ser informado o responsável para que dê andamento ao pedido de acordo com o Processo Gestão de Clientes, sendo fechado o incidente. Caso não o consiga, deve escalar para a 3ª Linha. Caso o SLA da 2ª Linha esteja prestes a ser atingido, deverá ser notificado o Coordenador da Linha para que actue em conformidade.
	<u>Efectuar diagnóstico avançado e identificar solução</u> A 3ª Linha, com base na informação disponível e com a que pode ainda obter do sistema ou aplicação, efectua uma análise e diagnóstico avançado com vista a determinar a solução definitiva do incidente. Sempre que exista um *workaround* que possa ser aplicado até que a solução seja encontrada e aplicada, este deve ser aplicado e registado na *Knowledge Base* (conforme actividade "Fechar o Incidente"). Em qualquer caso, se se verificar que já existe um problema registado, deverá ser feito o relacionamento dos registos. Caso se comprove haver relação causa-efeito entre a implementação de uma alteração e o incidente reportado, deverá proceder-se ao relacionamento dos respectivos registos. Em alguns casos, a 3ª Linha pode ser garantida por fornecedor externo, podendo ter que se ter em conta as respectivas condições contratuais. A solução pode originar a criação de um RFC (Pedido de manutenção correctiva). Nestas situações, o Cliente deve ser informado do tempo

	de execução da solução, mantendo-se o incidente em aberto até ser concluída a alteração. Caso se identifique que a solução passará por uma manutenção evolutiva deverá ser informado o responsável para que dê andamento ao pedido de acordo com o Processo Gestão de Clientes, sendo fechado o incidente. Caso o SLA da 3ª Linha esteja prestes a ser atingido, deverá ser notificado o Coordenador da Linha para que actue em conformidade
Ferramentas de Suporte	
• *Knowledge Data Base* (Gestão de Incidentes, Gestão de Alterações, Gestão de Configurações)	

3.4.4. Resolver e Validar

Actividade	Resolver e Validar
Objectivos	Repor o serviço através da aplicação da solução encontrada e obter a respectiva validação da eficácia junto do cliente.
Papéis e Responsabilidades	• Cliente – Validar se o serviço voltou ao normal; Classificar a sua satisfação com a resolução do incidente. • 1ª, 2ª ou 3ª Linha – Repor o serviço, usando a solução encontrada; Validar com o cliente (no caso da 1ª Linha) ou tecnicamente a reposição do serviço; Registar a utilização da solução.
Inputs	• Incidente actualizado com detalhe (*activity log*, etc.) • *Knowledge Data Base* de soluções
Outputs	• Resposta do RFC (Pedido de manutenção correctiva ou evolutiva) (se aplicável) (output intermédio). • Solução utilizada. • Incidente validado pelo Cliente. • Classificação de satisfação atribuída pelo Cliente. • Serviço reposto.

Tarefas	Resolver o incidente De acordo com a Linha que identificou a solução a aplicar, esta deve efectuar os respectivos procedimentos e resolver o incidente. Deve também registar a utilização da solução se esta já existir na *Knowledge Data Base*.
	Validar reposição do serviço Cada Linha ou fornecedor, após aplicação da solução, verifica, dentro das suas competências, a reposição do serviço. O Cliente é notificado da resolução do incidente, devendo validar a reposição do serviço e classificar a sua satisfação com a resolução do incidente.
Ferramentas de Suporte	
• *Knowledge Data Base* (Gestão de Incidentes, Gestão de Alterações)	

3.4.5. Fechar o Incidente

Actividade	Fechar o Incidente
Objectivos	Efectuar os procedimentos necessários ao fecho do incidente.
Papéis e Responsabilidades	• 1ª, 2ª ou 3ª Linha – Actualizar documentação / informação associada ao incidente; Propor o registo na *Knowledge Data Base* da solução utilizada (não aplicável à 1ª Linha). • 1ª Linha – Fechar o incidente e outros registos associados, se existirem. • Cliente – Aceitar o fecho do incidente.
Inputs	• Incidente validado pelo Cliente. • *Knowledge Data Base* de soluções.
Outputs	• Incidente fechado. • Proposta de *workaround* / solução definitiva para *Knowledge Base* de soluções.

	• Documentação das aplicações / sistemas actualizada. • RFC para actualização da CMDB (se aplicável).
Tarefas	Actualizar documentação/informação associada A respectiva Linha que resolveu o incidente, deve actualizar documentação do sistema ou aplicação, bem como propor o registo de novas soluções, criando sempre que possível procedimentos para que as Linhas anteriores possam resolver incidentes semelhantes. Devem também ser actualizadas soluções anteriormente registadas para as quais se tenha detectado algum erro, incluindo as que se verificaram não terem sido eficazes.
	Fechar registos Efectuar o respectivo fecho na ferramenta de suporte. O Cliente deve aceitar este fecho.
Ferramentas de Suporte	
• *Knowledge Data Base* (Gestão de Incidentes, Gestão de Alterações, Gestão de Problemas, Gestão de Indisponibilidades, Gestão de Configurações)	

3.4.6. Monitorizar, Controlar e Comunicar

Actividade	Monitorizar, Controlar e Comunicar
Objectivos	Monitorizar e controlar incidentes cuja gravidade, volume, etc., justifiquem intervenção do Gestor de Incidentes e necessitem de maior cuidado na comunicação com o Cliente.
Papéis e Responsabilidades	• Gestor de Incidentes – Controlar/coordenar casos graves, de grande volume, situações em que não se conhece o correcto encaminhamento para 2ª ou Linhas e/ou haja necessidade de envolvimento de várias equipas de 2ª ou de 3ª Linha, sem que nenhuma delas assuma a responsabilidade sobre a resolução do incidente; Escalar hierarquicamente, quando necessário; Registar problemas e anomalias graves, quando são detectados pela 1ª ou 2ª Linhas ou que o próprio identifique sem que haja já registo criado.

Inputs	• Registos de Incidentes.
Outputs	• Relatórios de gestão com progresso de incidentes. • Relatórios / Comunicação para Cliente. • Registo de problema (se aplicável). • Registo de anomalia grave (se aplicável).
Tarefas	<u>Monitorar e coordenar incidentes</u> O Gestor de Incidentes deve monitorizar regularmente o estado e progresso da resolução dos incidentes abertos, tendo em conta os níveis de serviço definidos para cada Linha. Sempre que lhe seja solicitado, deve apoiar a classificação de um incidente, para que o seu encaminhamento seja o correcto. Deve identificar os incidentes para os quais é necessário coordenação/controlo mais apertado (gravidade, "saltos" entre equipas, etc.). Coordenar e escalar, sempre que se justifique. Deve ainda identificar incidentes semelhantes, ou analisar os alertas de potenciais problemas que lhe são enviados pela 1ª ou 2ª Linhas, e registar o problema, se for o caso, se este ainda não tiver sido registado, e relacioná-lo com o incidente. Deve também efectuar o registo de uma anomalia grave e relacioná-lo com o incidentes, caso identifique que o impacto do incidente em termos financeiros e/ou reputacionais é considerável e as suas consequências extravasam o âmbito.
	<u>Comunicar com o Cliente</u> O Gestor de Incidentes, para os incidentes mais críticos, com maior impacto e visibilidade para os Clientes e para o negócio, deve manter o Cliente informado do progresso da resolução desses incidentes, recebendo ou tendo acesso a toda a informação que seja relevante e necessária para efectuar essa comunicação.
Ferramentas de Suporte	
• *Knowledge Data Base* (Gestão de Incidentes, Gestão de Problemas)	

3.5. Métricas de Qualidade de Serviço e Indicadores do Processo

Objectivos	Indicadores	Métricas
Reposição do serviço no mais curto espaço de tempo possível e com o objectivo de criar o mínimo impacto adverso no negócio.	I_{1n} = Percentagem de incidentes resolvidos na n-ésima Linha $I_{1n} = \frac{A_n}{B} \times 100$	A_n = nº de incidentes resolvidos pela n-ésima Linha n = 1, 2, 3 B = nº de incidentes registados
	I_2 = Percentagem de incidentes reabertos $I_2 = \frac{C}{D} \times 100$	C = nº de incidentes reabertos D = nº de incidentes resolvidos
	I_{3j} = Duração média dos incidentes por prioridade j $I_{3j} = \frac{\sum_{i=1}^{D} E_{ij}}{D}$	E_{ij} = duração do incidente i de prioridade j j = Alta, Média, Baixa
	I_4 = Tempo médio de reacção aos incidentes $I_4 = \frac{\sum_{i=1}^{D} G_i}{D}$	G_i = tempo de reacção ao incidente i, ou seja, desde que o incidente i é registado até que se inicie o seu tratamento
	I_5 = Tempo médio de resolução dos incidentes $I_5 = \frac{\sum_{i=1}^{D} H_i}{D}$	H_i = tempo de resolução do incidente i, ou seja, desde que se inicia o seu tratamento até que esteja resolvido

Objectivos	Indicadores	Métricas
Assegurar que os melhores níveis possíveis de qualidade e disponibilidade do serviço se mantêm	I_1 = Grau de satisfação médio dos clientes com a resolução dos incidentes $I_1 = \frac{\sum_{i=1}^{B} A_i}{B}$	A_i = classificação de satisfação com a resolução atribuída ao incidente i B = nº de incidentes com classificação de satisfação atribuída pelo cliente
	I_2 = Percentagem de incidentes resolvidos dentro do tempo acordado / aceitável $I_2 = \frac{C}{D} \times 100$	C = nº de incidentes resolvidos dentro do tempo acordado / aceitável D = nº de incidentes resolvidos

Tabela 3.2 - Métricas e Indicadores do Processo

3.6. Relação do Processo com Normas e Boas Práticas

O processo de gestão de incidentes anteriormente apresentado, demonstra uma implementação seguindo as boas práticas do ITIL, assim como um nível de maturidade do *CobiT* que corresponde ao critério exigido pelo Basileia II, procurando a melhoria continua com o recurso a métricas de qualidade e a segurança permanente da informação.

3.7. Mapeamento do Processo de Gestão de Incidentes com o Modelo Dinâmico.

A tabela 3.3 apresenta o mapeamento do processo de gestão de incidentes descrito neste capítulo, no modelo dinâmico implementado.

Processo de Gestão de Incidentes	Modelo Dinâmico	Formulas e Indicadores (ANEXO VI)
Detectar incidentes	Incidentes e Eventos	Incidentes e Eventos
Classificar o Incidente	Qualidade da Investigação	Qualidade da Investigação
Analisar e Diagnosticar	Qualidade da Investigação	Qualidade da Investigação
Resolver e Validar	Motivação para Reportar	Motivação para Reportar Incidentes
Fechar o Incidente	Efeitos da Aprendizagem	Efeitos da Aprendizagem

Tabela 3.3 – Mapeamento do Processo com Modelo Dinâmico

4. EXECUÇÃO DA SIMULAÇÃO NO MODELO

4.1. Descrição do cenário

Nesta simulação é assumido que já existe um sistema de aprendizagem de incidentes aquando do início da simulação. O modelo está, portanto, inicializado em equilíbrio. A gestão tem, ao início, toda a atenção posta na notificação de incidentes, tendo a percepção da sua importância. "*Management Focus on Incidents*" é inicialmente igual a 1. A notificação de eventos é percepcionada como sendo menos importante, tendo portanto um valor de 0,25.

Embora a gestão se concentre na notificação de incidentes, o ambiente de notificação não é o melhor. "*Effectiveness of Recriminations*" tem um valor de 1. Também existe um esquema de incentivos. *"Effectiveness of Incentives"* tem um valor inicial de 1.

A área em estudo para este trabalho, apresenta um valor mensal de 427 eventos.

Foram analisados seis cenários diferentes, identificados na **tabela 4.1**, a que correspondem valores iniciais diferentes para as variáveis exógenas indicadas.

Cenário Nº	**Nome do Cenário**	**Incremento dos Incentivos**	**Redução das Recriminações**	**Investigações Inadequadas**	**Management Focus nos Eventos**
1	Redução das Recriminações		**X**		
2	Incremento dos Incentivos	**X**			
3	Recursos Inadequados			**X**	
4	Man.Focus Eventos				**X**
5	Man.Focus Eventos – Redução das Recriminações		**X**		**X**

Cenário Nº	Nome do Cenário	Incremento dos Incentivos	Redução das Recriminações	Investigações Inadequadas	Management Focus nos Eventos
6	Man.Focus Eventos – Incremento dos Incentivos	**X**			**X**

Tabela 4.1 – Cenários propostos para a simulação

4.2. Variáveis da simulação

As tabelas 4.2 a 4.7 detalham os valores utilizados na simulação dos vários cenários.

Cenário nº 1 – Redução das Recriminações			
Variáveis do Modelo	**Descrição da Simulação**	**Valores Iniciais**	**Valores de Simulação**
Effectiveness of Recriminations	Redução das Recriminações em 75% a partir do 3º mês	1	1-STEP(0.75,3)
Effectiveness of Incentives		1	
Management Focus On Events		0.25	
Management Focus On Events – Recriminations			
Management Focus On Events – Incentives			
Hours Available		100	

Tabela 4.2 – Variáveis do cenário "Redução das Recriminações"

Cenário nº 2 – Incremento dos Incentivos			
Variáveis do Modelo	**Descrição da Simulação**	**Valores Iniciais**	**Valores de Simulação**
Effectiveness of Recriminations		1	
Effectiveness of Incentives	Incremento dos Incentivos em 75% a partir do 3º mês	1	1+STEP(0.75,3)
Management Focus On Events		0.25	
Management Focus On Events - Recriminations			
Management Focus On Events - Incentives			
Hours Available		100	

Tabela 4.3 – Variáveis do cenário "Incremento dos Incentivos"

Cenário nº 3 – Recursos Inadequados			
Variáveis do Modelo	**Descrição da Simulação**	**Valores Iniciais**	**Valores de Simulação**
Effectiveness of Recriminations		1	
Effectiveness of Incentives		1	
Management Focus On Events		0.25	
Management Focus On Events - Recriminations			
Management Focus On Events - Incentives			
Hours Available	Redução dos Recursos para 95% das necessidades	100	1-STEP(96,3)

Tabela 4.4 – Variáveis do cenário "Recursos Inadequados"

Cenário nº 4 – Management Focus Eventos (MFE)			
Variáveis do Modelo	**Descrição da Simulação**	**Valores Iniciais**	**Valores de Simulação**
Effectiveness of Recriminations			
Effectiveness of Incentives			
Management Focus On Events	Igual importância dada pela gestão dos eventos	0.25	0.25+STEP(0.75,3)
Management Focus On Events - Recriminations		1	
Management Focus On Events - Incentives		1	
Hours Available		100	

Tabela 4.5 – Variáveis do cenário "Management Focus Eventos"

Cenário nº 5 – Management Focus Eventos (MFE) - Redução das Recriminações			
Variáveis do Modelo	**Descrição da Simulação**	**Valores Iniciais**	**Valores de Simulação**
Effectiveness of Recriminations			
Effectiveness of Incentives			
Management Focus On Events	Igual importância dada pela gestão dos eventos	0.25	0.25+STEP(0.75,3)
Management Focus On Events - Recriminations	Redução das Recriminações em 75% a partir do 3º mês	1	1-STEP(0.75,3)
Management Focus On Events - Incentives		1	
Hours Available		100	

Tabela 4.6 – Variáveis do cenário "MFE – Redução das Recriminações"

Cenário nº 6 – Management Focus Eventos (MFE) - Incremento dos Incentivos			
Variáveis do Modelo	**Descrição da Simulação**	**Valores Iniciais**	**Valores de Simulação**
Effectiveness of Recriminations			
Effectiveness of Incentives			
Management Focus On Events	Igual importância dada pela gestão dos eventos	0.25	0.25+STEP(0.75,3)
Management Focus On Events - Recriminations		1	
Management Focus On Events - Incentives	Incremento dos Incentivos em 75% a partir do 3º mês	1	1+STEP(0.75,3)
Hours Available		100	

Tabela 4.7 – Variáveis do cenário "MFE – Incremento dos Incentivos"

4.3. Apresentação e análise dos resultados

Nesta secção são apresentados os resultados obtidos com a simulação no modelo de Gestão de Incidentes, variando o tipo de cenário e os valores já descritos na secção anterior (**Figura 4.1 a Figura 4.12**).

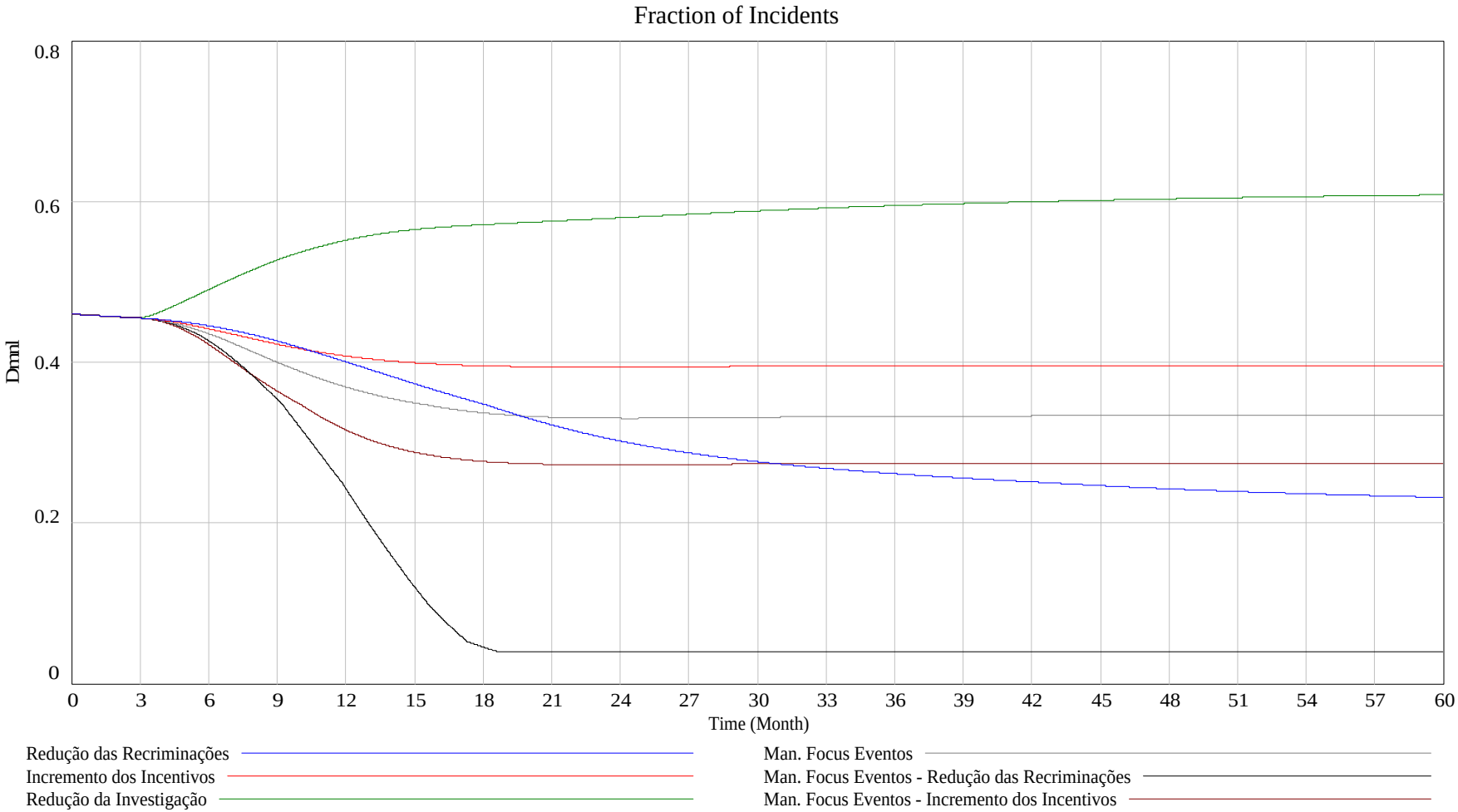


Figura 4.1 - Simulação “Fraction of Incidents”

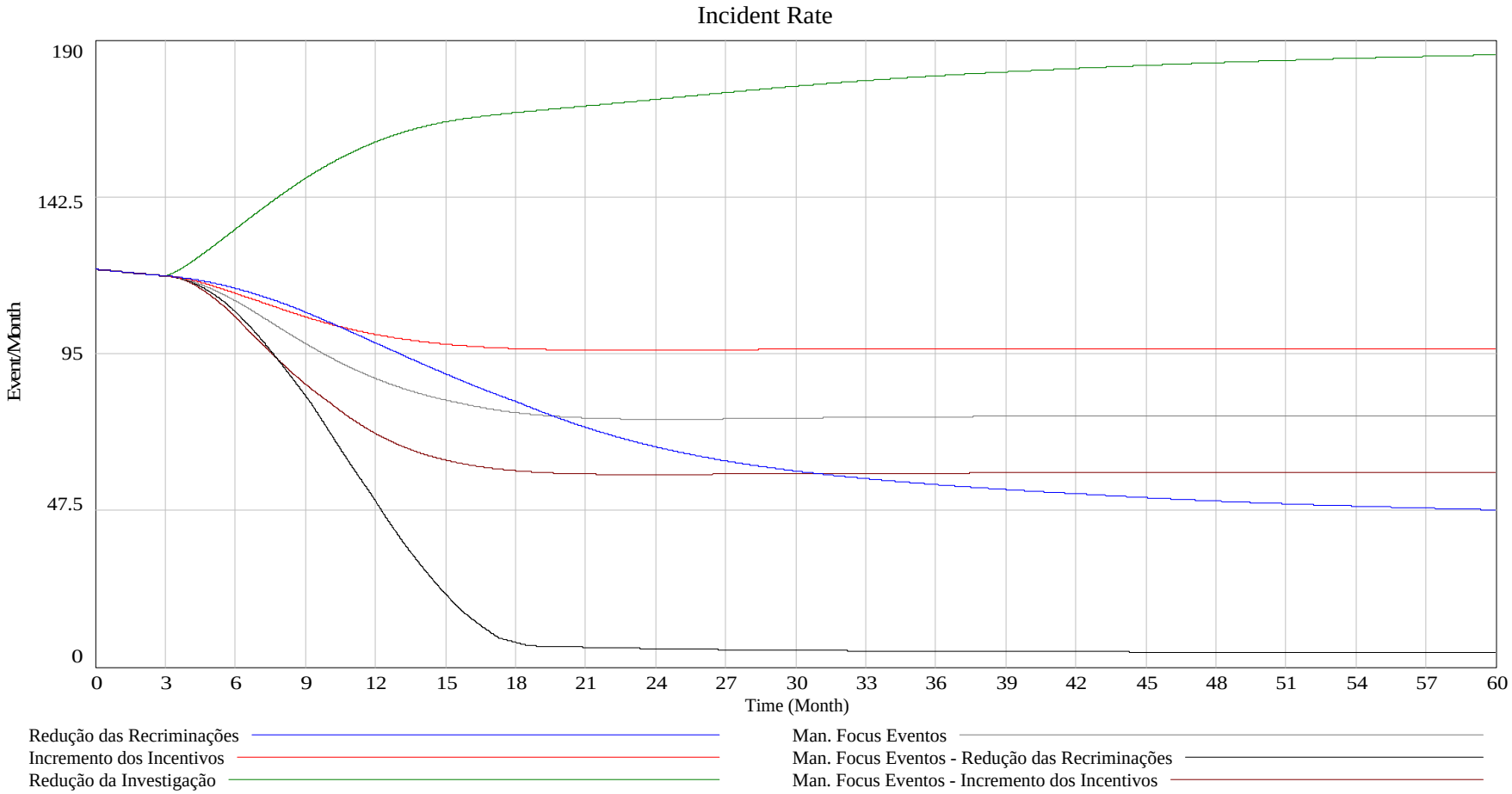


Figura 4.2 - Simulação “Incident Rate”

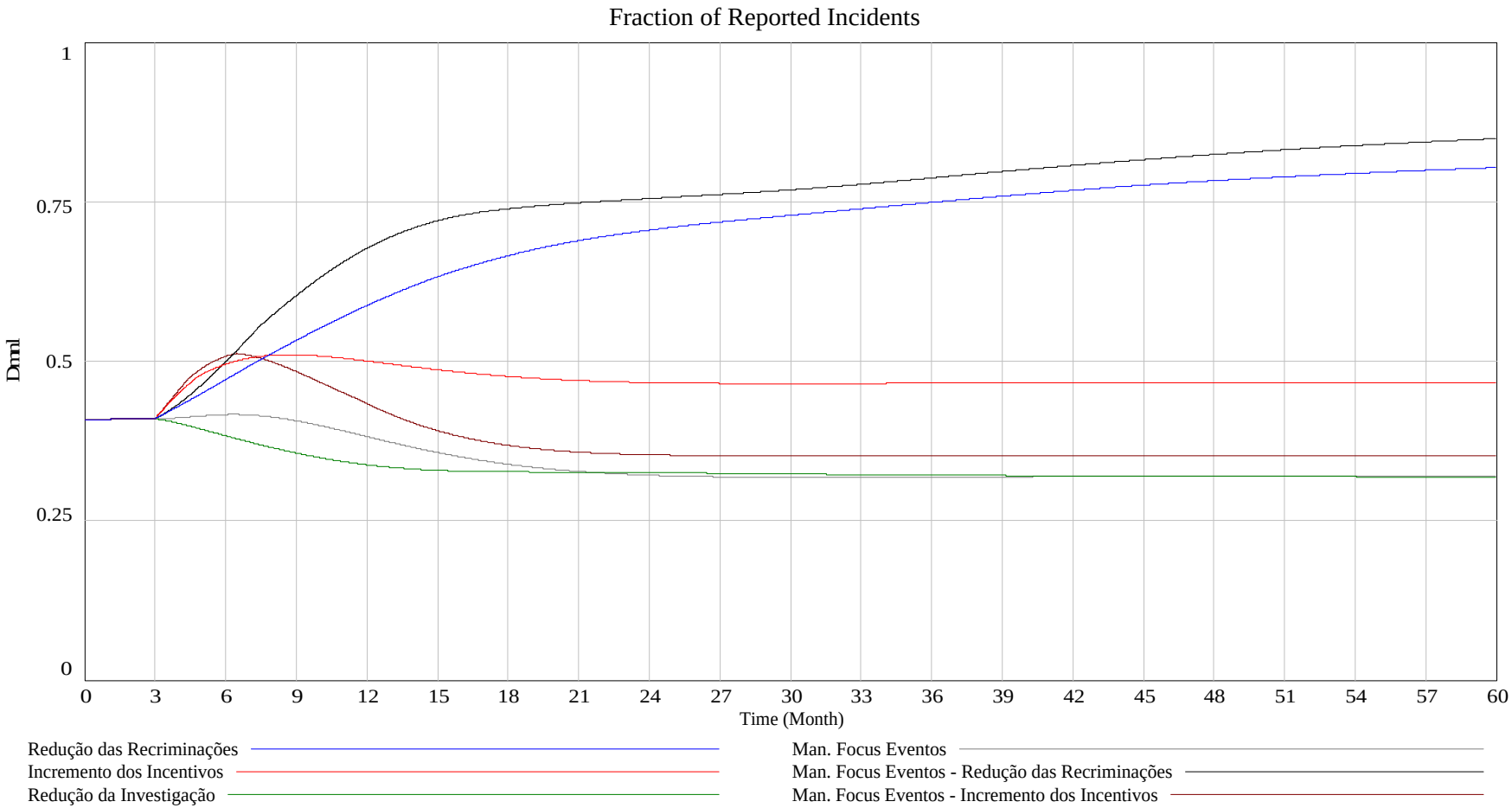


Figura 4.3 - Simulação "Fraction of Reported Incidents"

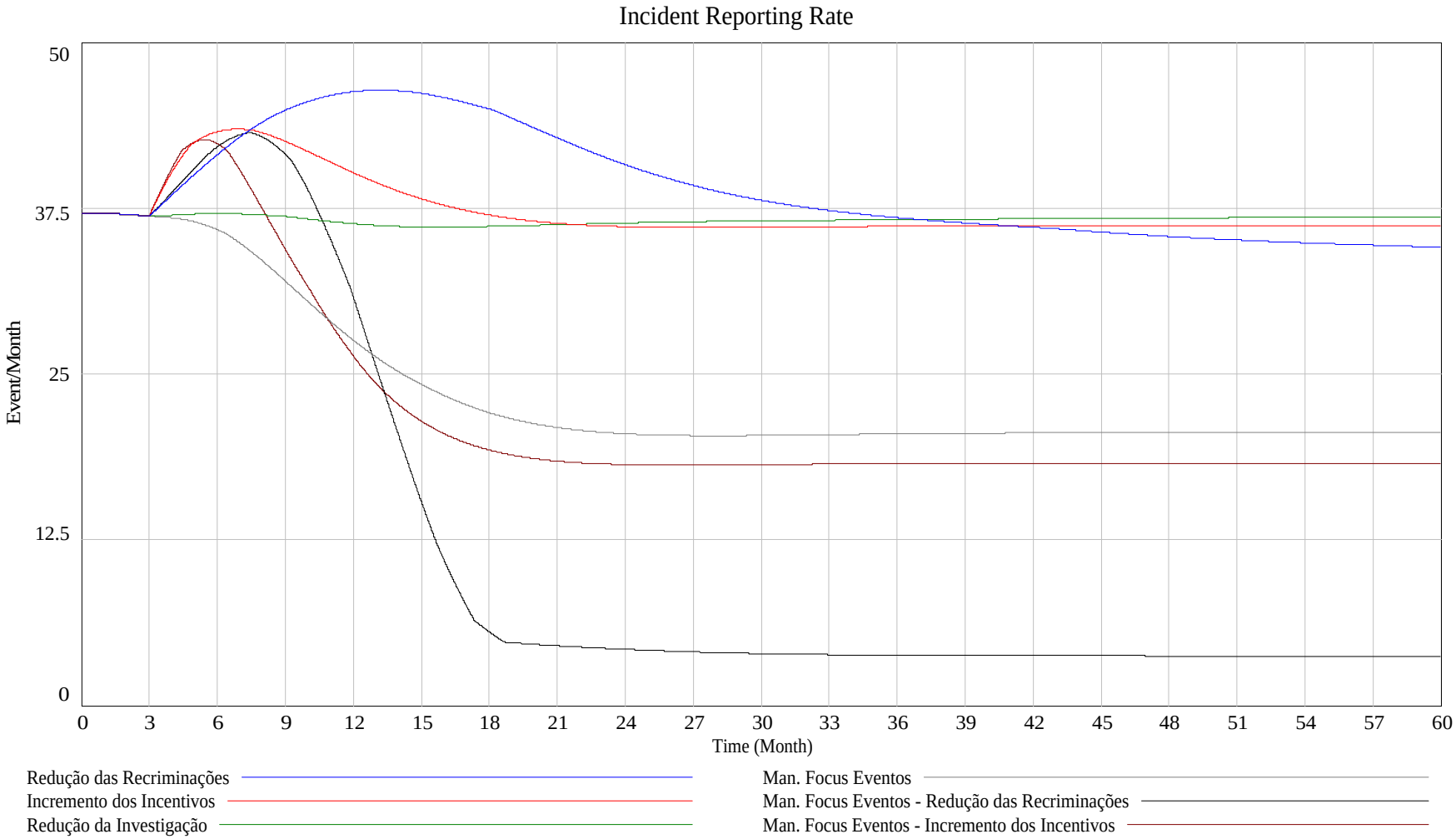


Figura 4.4 – Simulação "Incident Reporting Rate"

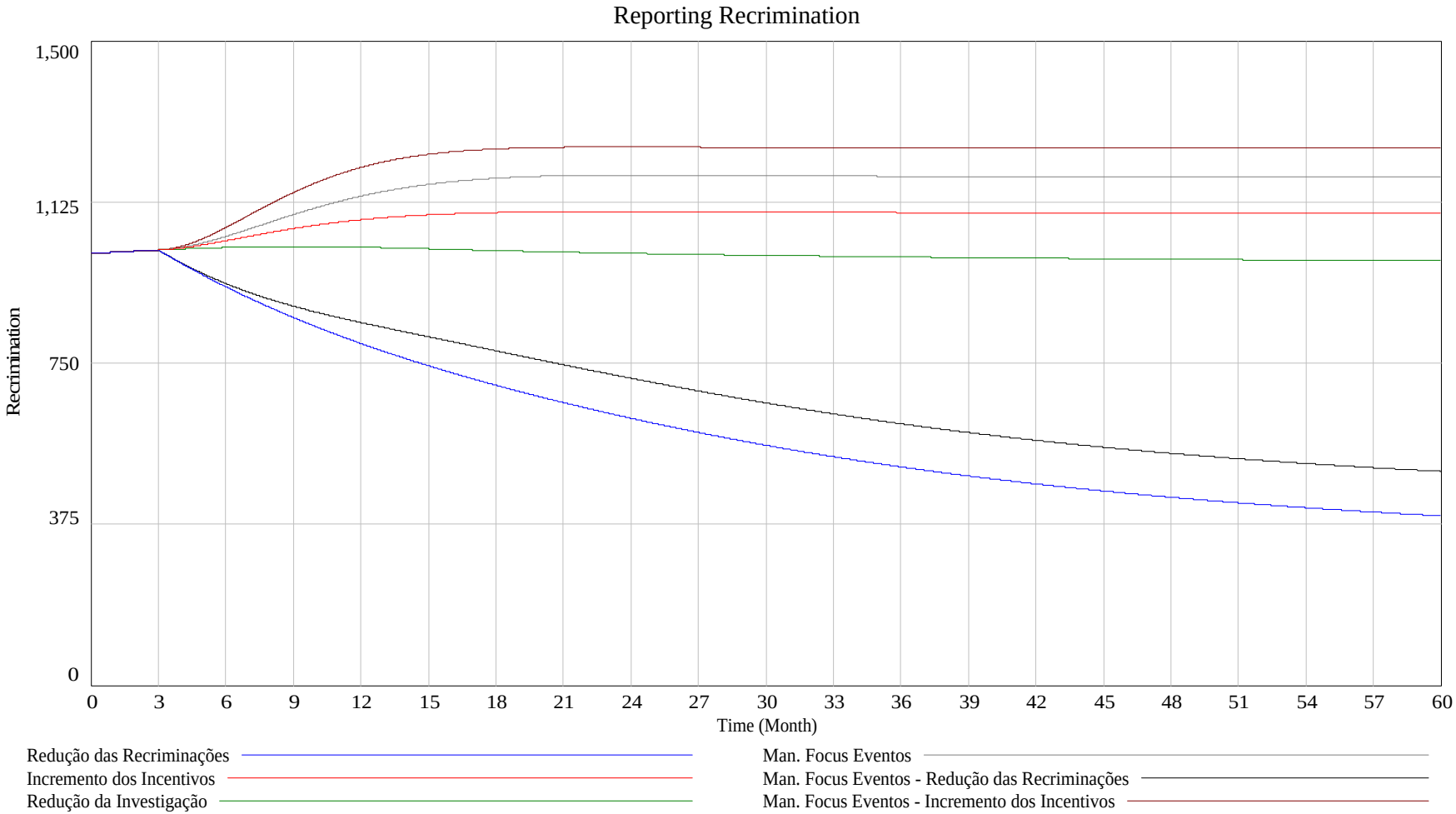


Figura 4.5 – Simulação "Reporting Recriminations"

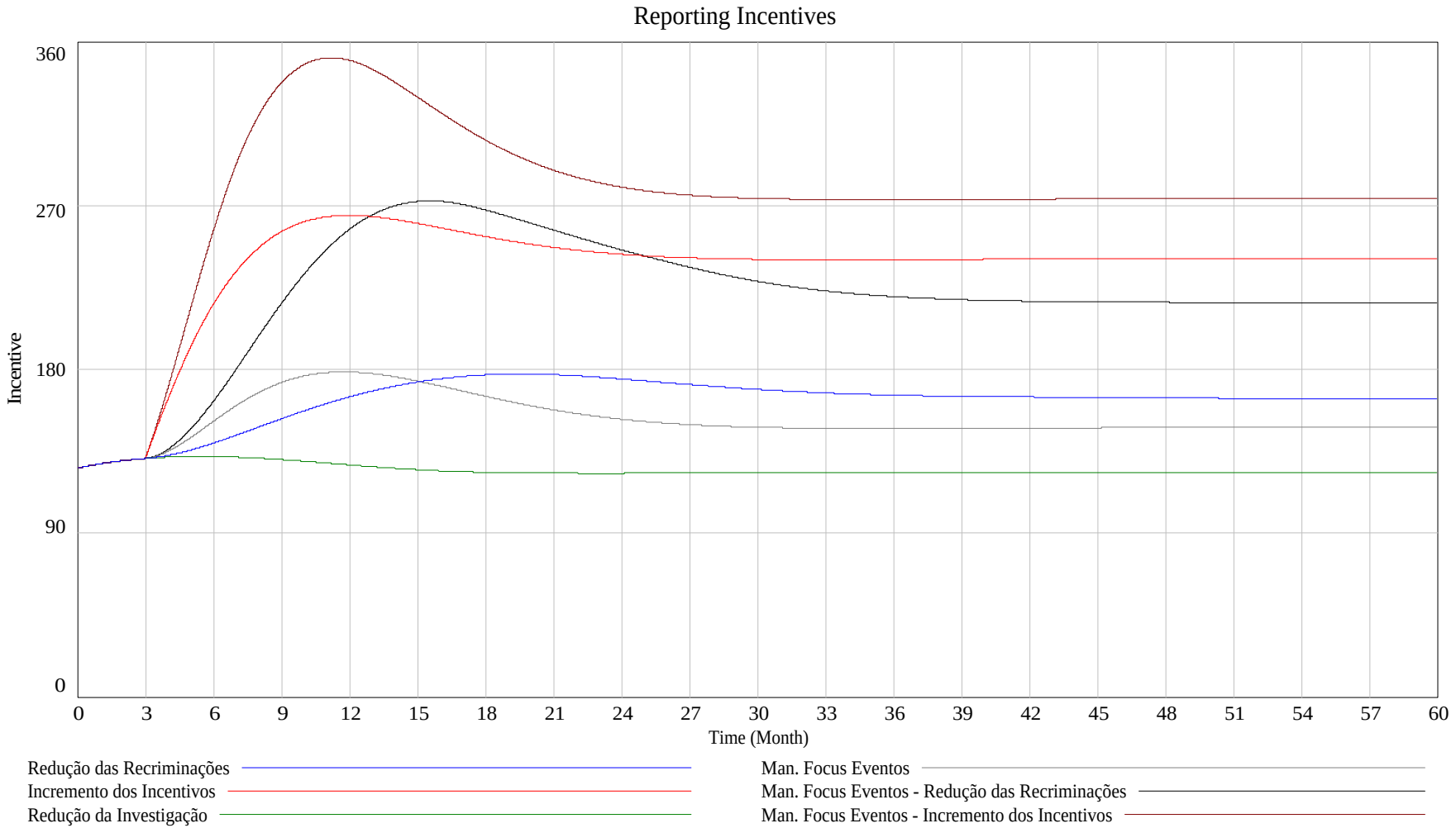


Figura 4.6 – Simulação "Reporting Incentives"

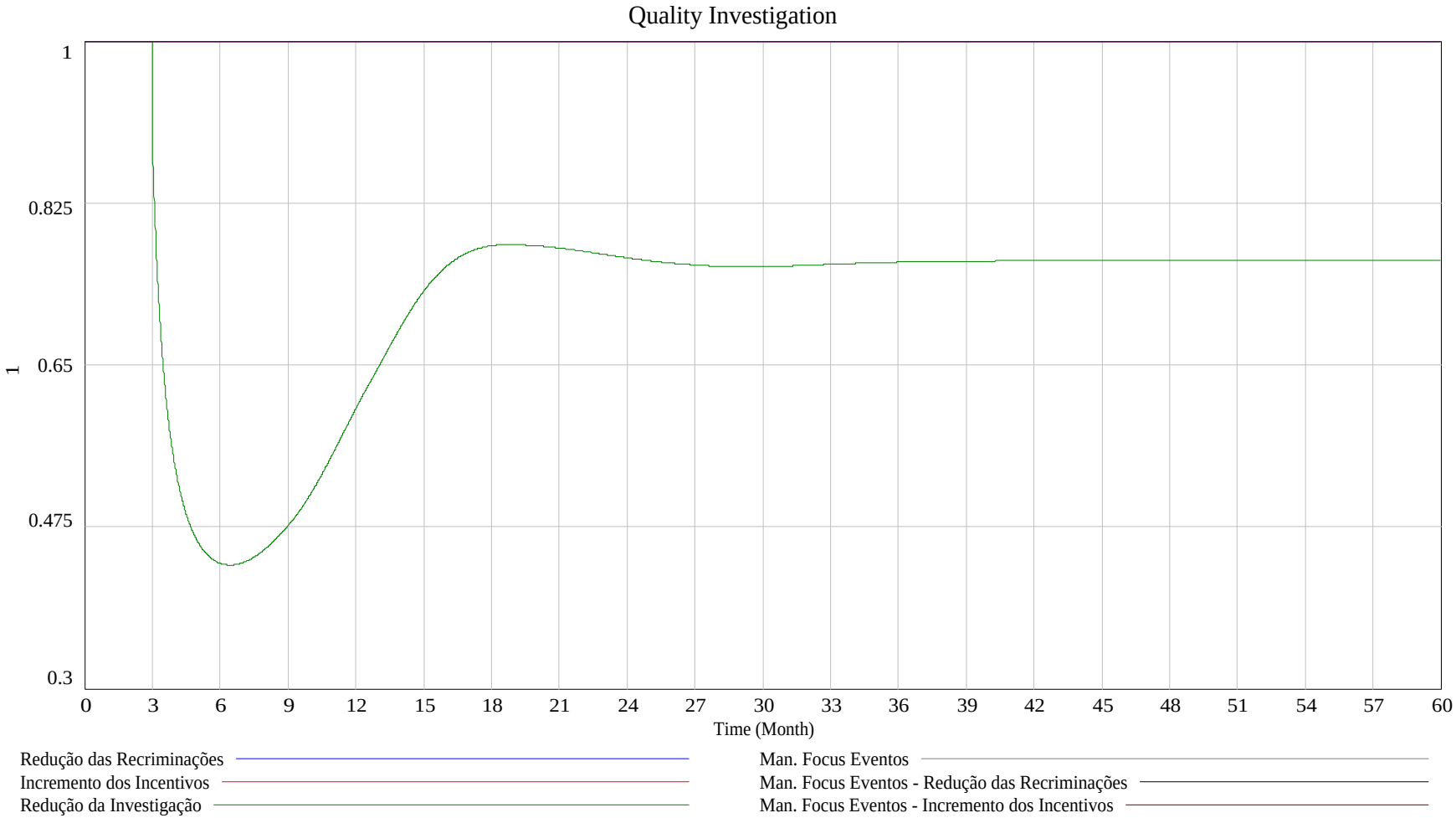


Figura 4.7 – Simulação "Quality of Investigation"

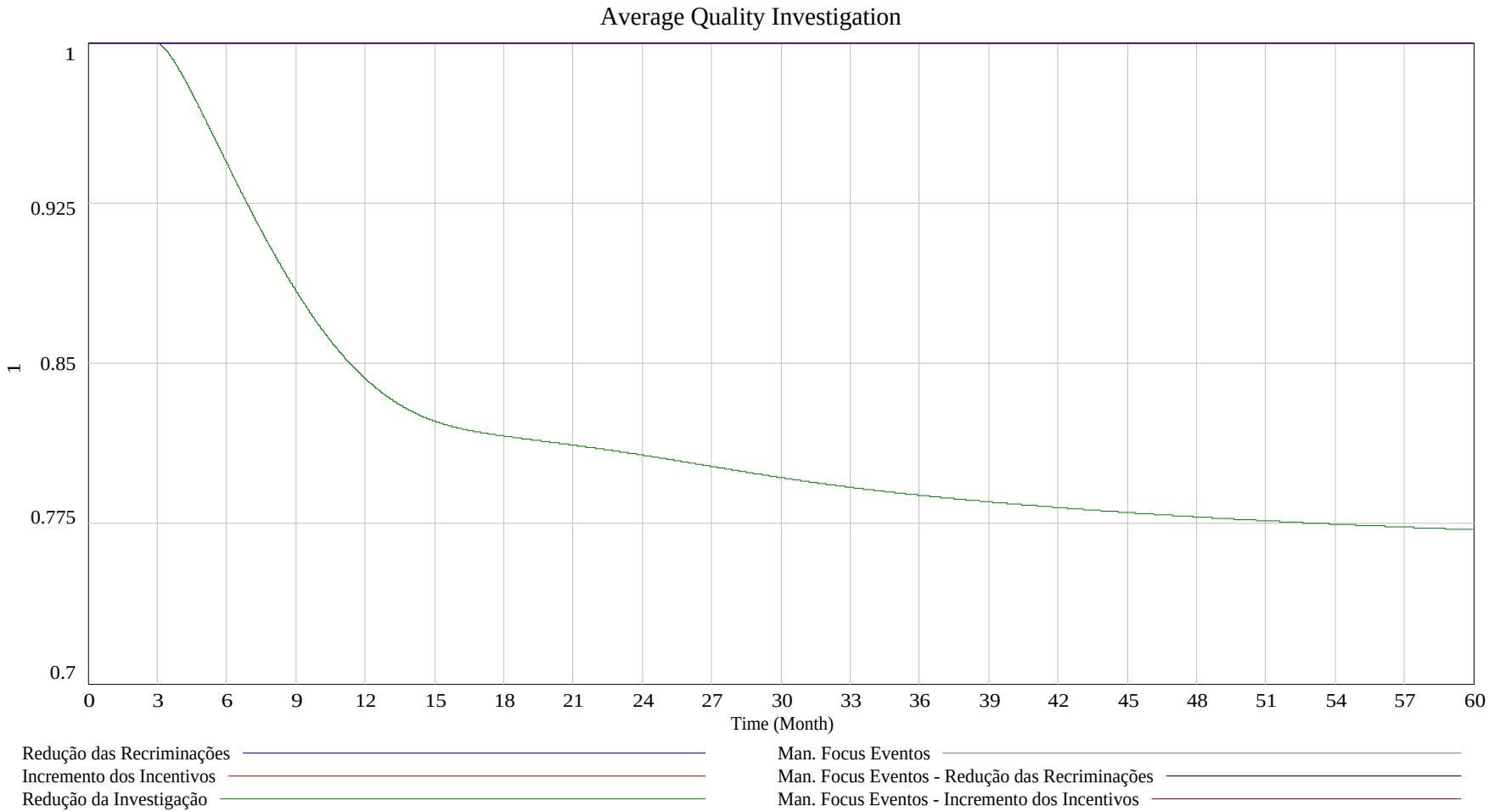


Figura 4.8 – Simulação "Average Quality of Investigation"

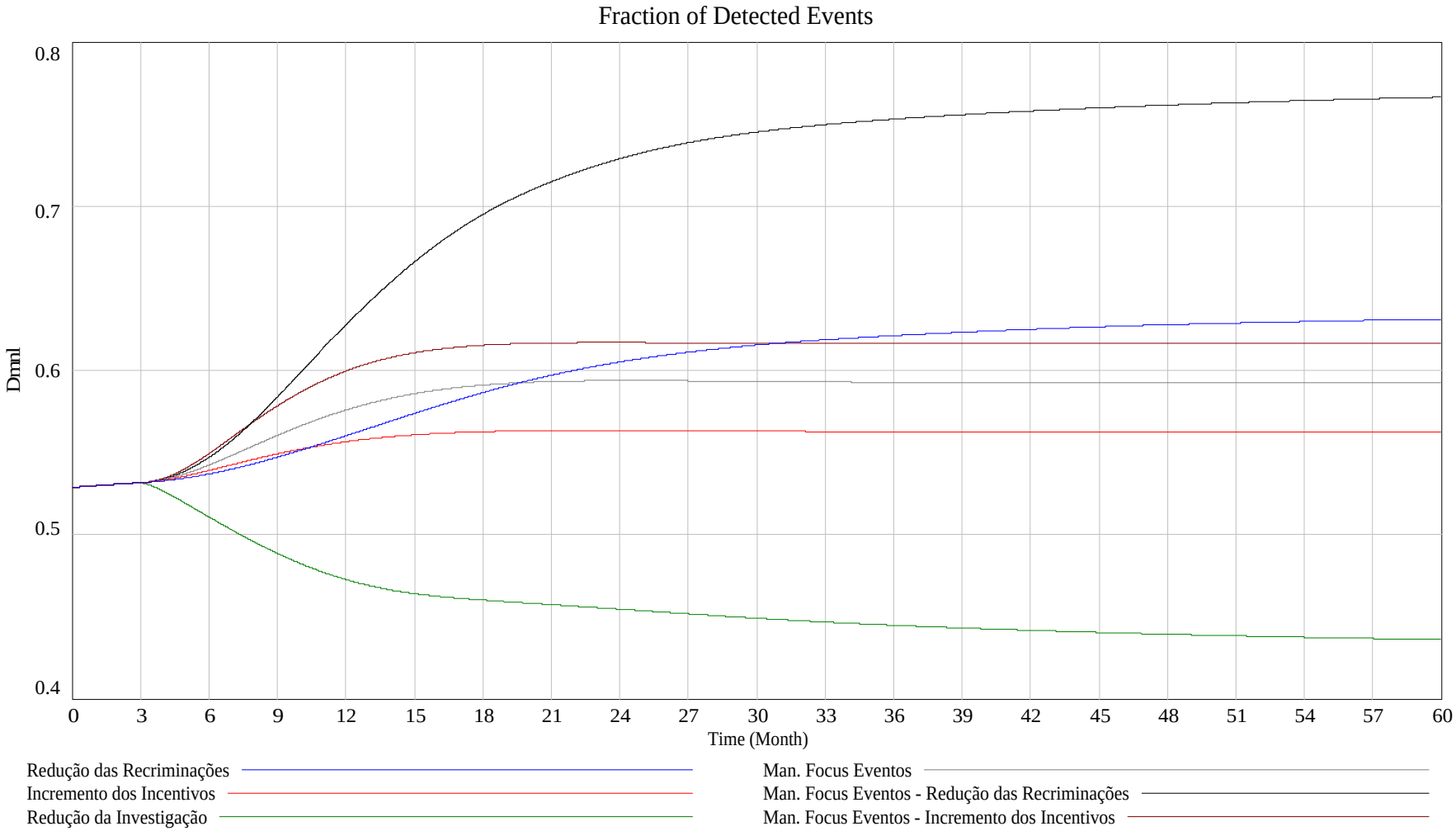


Figura 4.9 – Simulação "Fraction of Detected Events"

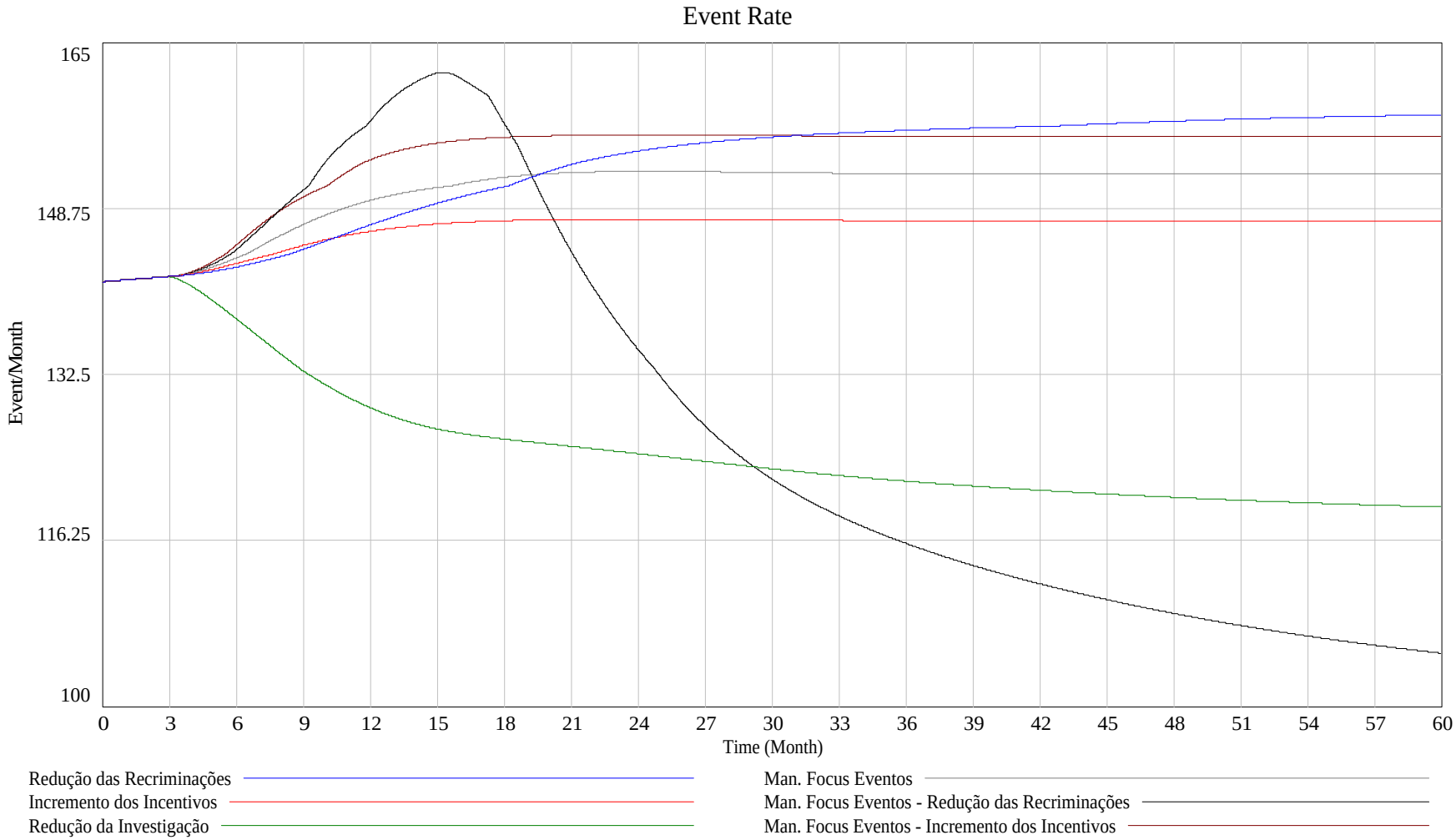


Figura 4.10 – Simulação "Event Rate"

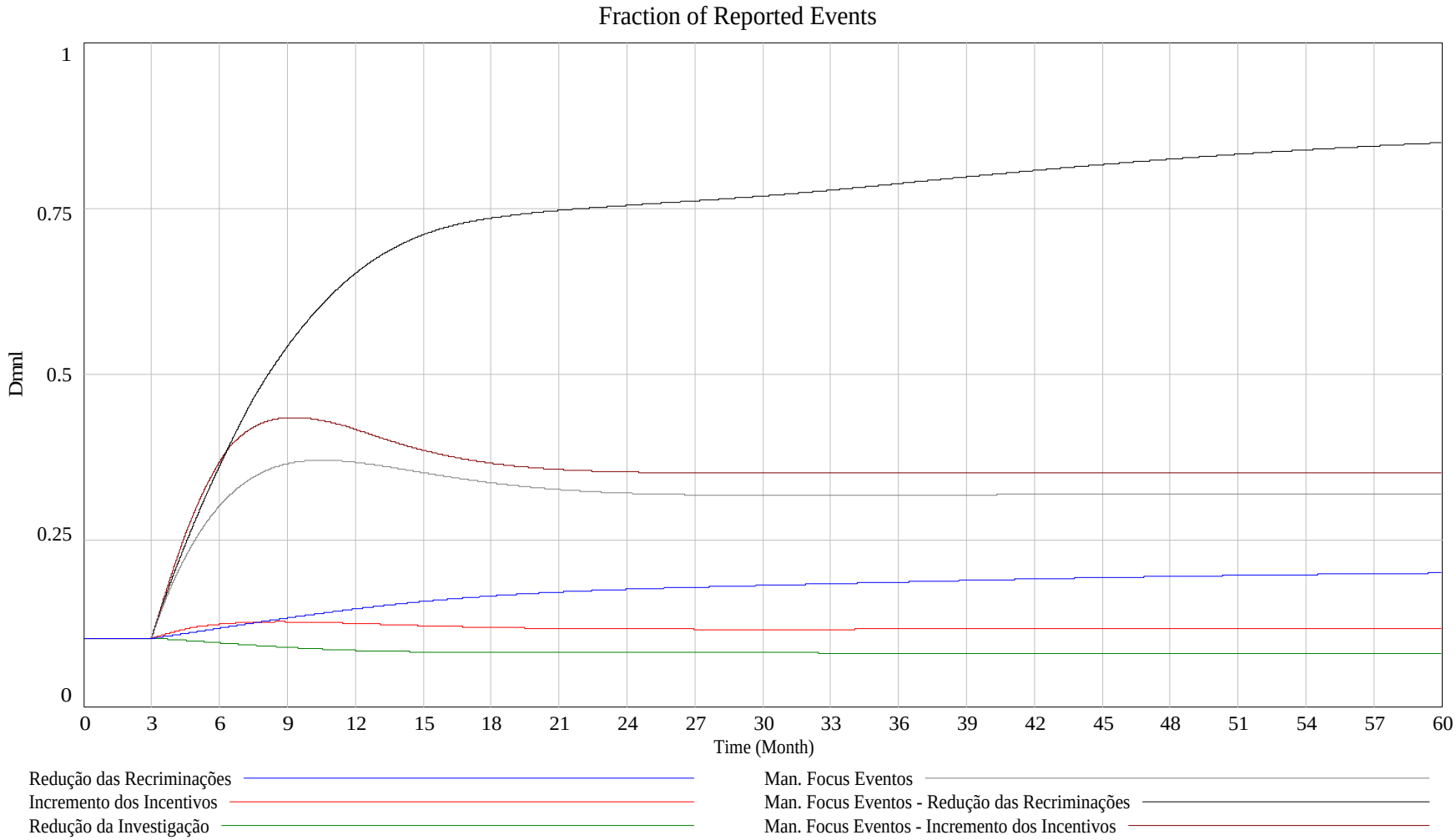


Figura 4.11 – Simulação "Fraction of Reported Events"

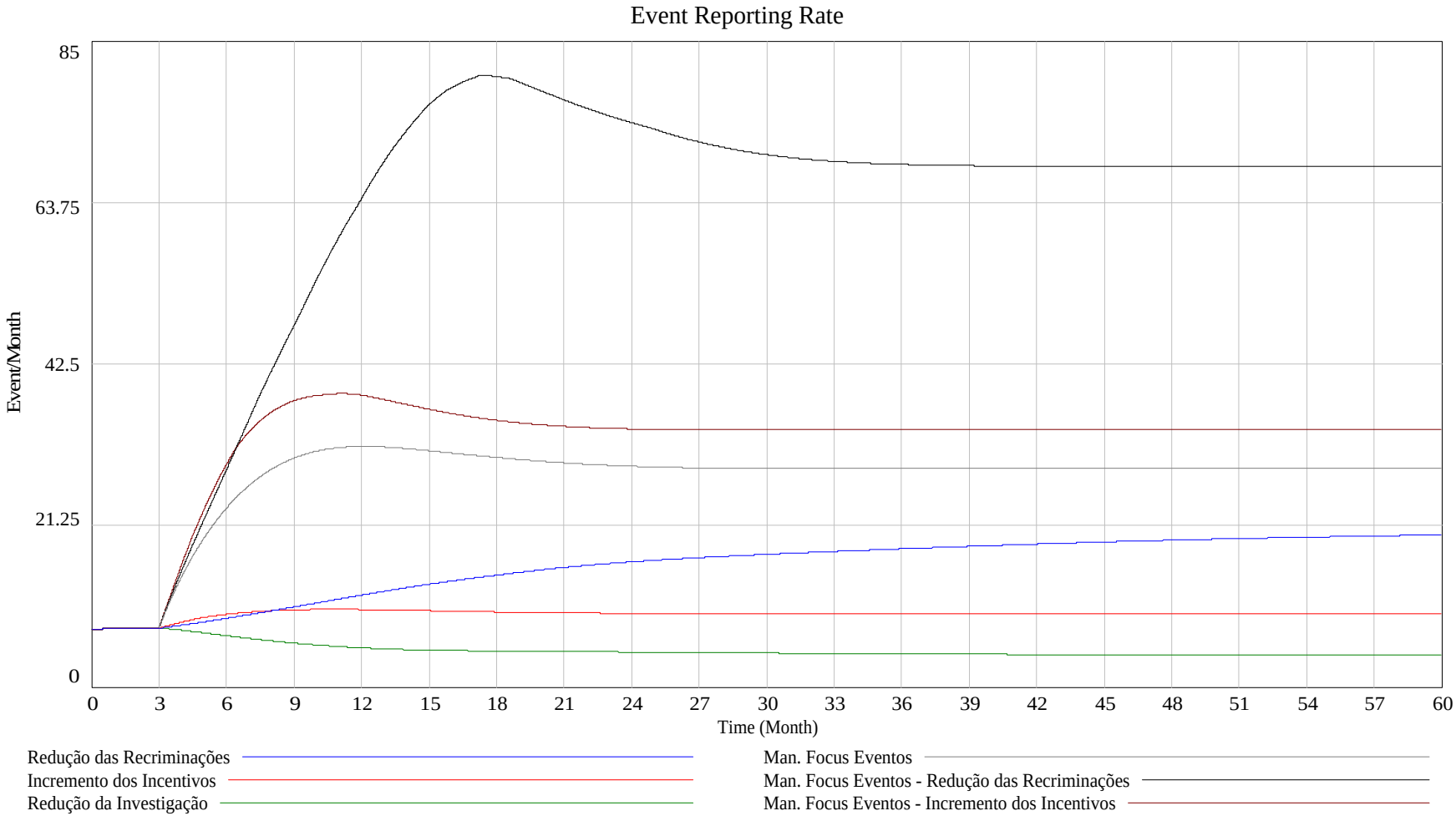


Figura 4.12 – Simulação "Event Reporting Rate"

4.3.1. Incentivos e Recriminações

No cenário "Redução das Recriminações" a eficácia das recriminações é reduzida em 75% a partir do terceiro mês. Contudo as recriminações não são completamente reduzidas, dado que poderão existir vários factores que determinarão a ocorrência ou não de recriminações. Por exemplo, mesmo que a gestão consiga eliminar as suas recriminações, poderá ainda existir alguma 'pressão dos pares' por parte de colegas.

Na simulação "*Fraction of Incidents*" **(Figura 4.1)**, este cenário desce gradualmente ao longo da simulação. Na simulação "*Fraction of Reportes Incidents*" **(Figura 4.3)**, mostra um comportamento inverso, aumentando gradualmente. Este comportamento divergente de "*Fraction of Incidents*" **(Figura 4.1)** e de "*Fraction of Reportes Incidents*" **(Figura 4.3)** tem uma consequência importante. Como apresentado, *"Incident Reporting Rate"* **(Figura 4.4)** aumenta durante doze meses, antes de gradualmente cair para um nível ligeiramente abaixo dos "Incrementos dos Incentivos". A redução de *"Incident Rate"* **(Figura 4.2)** não é directamente visível, dado que a gestão não tem acesso a este índice. Apenas podem fazer uma estimativa com base naquilo que é de facto reportado.

No Cenário "Incremento dos Incentivos" verifica-se um aumento na eficácia dos incentivos em 75% a partir do terceiro mês. Inicialmente existe um decréscimo gradual em "*Fraction of Incidents*" **(Figura 4.1)**. Todavia, após um período de cerca de 15 meses, o comportamento estabiliza. "*Fraction of Reportes Incidents*" **(Figura 4.3)** aumenta e atinge um pico no mês 9, após o qual desce ligeiramente. Este comportamento é causado por uma acumulação de recriminações. À medida que são reportados mais incidentes, maior é a acumulação de recriminações, limitando melhorias em *"Incident Rate*" **(Figura 4.2)**. Embora exista uma melhoria, esta não é visível neste momento.

4.3.2. Recursos Inadequados

No cenário "Recursos Inadequados", no mês 3, os recursos de investigação são reduzidos inicialmente para 95% daquilo que é necessário. Um 'log' de incidentes não investigados começa a crescer, causando uma carga de trabalho ainda maior. A qualidade da investigação é reduzida para que os incidentes possam ser processados mais rapidamente. A queda de *"Average Quality of Investigation"* **(Figura 4.8)** reflecte-se em "manter a equipa em efeito de ciclo". Subsequentemente, entram menos notificações, como se pode ver na queda de *"Fraction of Reported Incidents"* **(Figura 4.3)**.

Dado que as lições aprendidas são agora menos, o índice *"Fraction of Incidents"* **(Figura 4.1)** aumenta. Embora este aumento seja substancial, é afectado por uma baixa em *"Fraction*

of Reported Incidents" **(Figura 4.3)**, sendo que apenas se pode ver um pequeno aumento em *"Incident Reported Rate"* **(Figura 4.4)**. Uma situação que se tornou muito pior de que se poderia esperar, dado que muito pouco foi alterado.

4.3.3. Enfoque da Gestão aos Eventos – (Management Focus on Events)

As três execuções anteriores focaram-se na mudança de condições básicas de notificação de incidentes, analisando agora a notificação de eventos. Os cenários que se seguem simulam a promoção de notificação de eventos por parte da gestão de forma a estes terem o mesmo estatuto de notificação de incidentes. Nos cenários "Man. Focus Eventos", "Man. Focus Eventos – Redução das Recriminações " e "Man. Focus Eventos – Incremento dos Incentivos", o valor de "*Management Focus On Events*" é alterado de 0,25 para 1 a partir do terceiro mês.

No cenário "Man. Focus Eventos", uma atenção redobrada dada à notificação de eventos leva a um aumento por oito meses na simulação "*Event Reporting Rate*" **(Figura 4.12)**. Os eventos notificados representam mais lições aprendidas, sendo que como a base de aprendizagem é muito maior, "*Incident Rate*" **(Figura 4.2)** é reduzida. Todavia, e tal como no cenário "Incremento dos Incentivos", as recriminações começam a aumentar, à medida que entram mais notificações de eventos. Isto limita uma melhoria em "*Incident Rate*" **(Figura 4.2)**, que acaba por estabilizar após o mês 18.

A redução de '*Incident Rate*" **(Figura 4.2)** é acompanhada por *"Incident Reporting Rate*" **(Figura 4.4)**, não revelando no entanto optimismo. Embora a quantidade de notificações esteja a diminuir, isto não se deve apenas a uma redução verificada na simulação "*Incident Rate*" **(Figura 4.2)**. Um aumento do enfoque nos eventos provoca um ligeiro aumento inicial na simulação "*Fraction of Reported Incidents*" **(Figura 4.3)**. Todavia, a acumulação de recriminações rapidamente inverte este desenvolvimento. Ao fim de algum tempo, "*Fraction of Reported Incidents*" **(Figura 4.3)** acaba por estabilizar muito abaixo do seu valor inicial. Pode-se, portanto, ser levado a crer que a melhoria é maior do que realmente é. Se combinarmos o aumento do enfoque com uma diminuição das recriminações, emerge algo favorável: o cenário "Man. Focus Eventos – Redução das Recriminações ". Tal como no cenário "Redução das Recriminações", há um aumento de '*Fraction of Reported Incidents*" **(Figura 4.3)**, causando igualmente um aumento inicial de "*Incident Reporting Rate*" **(Figura 4.4)**. Após cerca de oito meses, este aumento transforma-se num decréscimo e a queda continua até ao mês 21.

O índice 'Notificação de Incidentes' estabiliza bastante abaixo do que era inicialmente e isto reflectiu-se em "*Incident Reporting Rate*" **(Figura 4.4)**. A ausência de recriminações

combinada com uma maior base de aprendizagem fornecida pela notificação de eventos, criando um sistema altamente eficaz.

Fazer aumentar os incentivos em vez de reduzir as recriminações é acompanhado por um aumento de "*Incident Rate*" **(Figura 4.2)**. Todavia, também aqui uma acumulação de recriminações limita a redução. A melhoria é ainda maior do que simplesmente focarmo-nos unicamente nos incentivos sem ligarmos à notificação de eventos.

4.3.4. Efeitos das Recriminações

Embora os incentivos possam parecer uma maneira rápida e fácil de melhorar a notificação de incidentes e de eventos **(Figura 4.5)**, os cenários "Incremento dos Incentivos" e "Man. Focus Eventos – Incremento dos Incentivos" mostram que aumentar os incentivos sem um trabalho de melhoria, clima de disponibilidade para a notificação poderá ser pouco sensato. Um programa de incentivos, que pode ser oneroso, pode-se revelar ineficaz, se não forem eliminadas totalmente as políticas das recriminações.

4.3.5. A Relação entre Incidentes e eventos

A comparação de "*Incident Reporting Rate*" **(Figura 4.4)** e de "*Event Reporting Rate*" **(Figura 4.12)** nas simulações anteriores revela comportamentos divergentes. Quantos mais eventos forem notificados, menos incidentes tendem a ser notificados. Isto é um efeito que foi demonstrado empiricamente por Jones, Kirchsteiger and Bjerke (1999). O modelo também mostra que na existência de políticas altamente eficientes que reduzam a sub-notificação, tanto os incidentes como os eventos podem aumentar durante algum tempo. Todavia, quando a sub-notificação tiver sido suficientemente reduzida, a redução dos incidentes propriamente ditos torna-se visível. Um estudo de duas fábricas Dinamarquesas apoia estes resultados. A introdução de um sistema de notificação de incidentes numa das fábricas levou a um aumento semestral na notificação de incidentes, seguido de um decréscimo até um nível mais baixo àquele que existia no momento da introdução. (Nielsen, Carstensen, e Rasmussen, 2006). Os autores atribuíram o aumento inicial a uma provável redução de sub-notificação.

4.3.6. Quantidade de Notificação de Incidentes como Indicador de Incidentes

Os cenários executados mostram que a quantidade de notificação de incidentes **(Figura 4.4)** é inadequada como único indicador de incidentes. Nos cenários "Redução das Recriminações" e "Incremento dos Incentivos", a quantidade de incidentes reportados acaba

por regressar a um valor estabilizado, enquanto a quantidade de incidentes **(Figura 4.2)** propriamente ditos acaba por ser mais baixa que o valor base.

No cenário "Recursos Inadequados", quase não se notam diferenças, embora a quantidade de incidentes esteja, na realidade, a aumentar.

No cenário "Man.Focus Eventos", uma melhoria na quantidade de incidentes pode ser notada através da quantidade de incidentes reportados, mas a magnitude da melhoria é "escondida" à medida que a fracção de notificação de incidentes baixa. Esta simulação mostra que é difícil usar a quantidade de incidentes como um indicador de melhoria ou não do sistema. Outros indicadores devem ser usados juntamente com as quantidades de notificação.

4.3.7. Lições aprendidas

Qual a importância das execuções anteriores da simulação? Não é a previsão exacta do que acontecerá num sistema específico de notificação. Pelo contrário, as execuções ilustram a compreensão estrutural contida no modelo **(Figura 2.16).** O conhecimento da estrutura do sistema e dos seus efeitos é crucial na capacidade do decisor em criar políticas que reduzem a quantidade e a gravidade dos incidentes.

As execuções da simulação ilustram o potencial de um sistema de notificação de incidentes de sucesso. Todavia, também mostram que existe a possibilidade de falha parcial, ou mesmo total, se factores importantes como a qualidade das investigações ou a motivação não forem bem geridos. Existe também a possibilidade de uma má avaliação do número de incidentes e eventos, se julgar que o número de incidentes e eventos é igual ao número de notificações. Um aumento ou decréscimo do número da notificação de incidentes pode ser bom ou mau e não é só por si um indicador de confiança no que diz respeito à segurança.

Os cenários da simulação indicam que a criação de uma cultura de segurança é possível. Uma cultura de segurança nasce quando um fluxo de notificações alimenta a tomada de consciência organizacional, aumentando-a ou mantendo-a num nível alto, de forma a permitir a detecção de novas situações de perigo ou a recaída na direcção de velhos e inseguros hábitos. No entanto, isto apenas é possível se as recriminações que se opõem à notificação forem minimizadas ou completamente removidas. Também têm de ser alocados à investigação recursos adequados.

5. CONCLUSÃO

O modelo dinâmico de um sistema de aprendizagem de segurança de incidentes e a literatura em que este se baseia mostra que há muitas dificuldades que têm de ser vencidas ao implementar sistemas de aprendizagem de incidentes completamente funcionais. O verdadeiro estado do sistema pode não ser aparente aos decisores, dado que o aumento das quantidades de notificação de incidentes tanto pode ser bom como mau e, em muitos casos, enganador. Não é, por isso, possível confiar exclusivamente na quantidade de notificação de incidentes. A relação entre quantidades de notificação de incidentes e de eventos pode ser um indicador do estado do sistema. Todavia, é igualmente necessário medir a cultura de segurança e o grau de severidade dos incidentes, uma vez que a queda na severidade dos incidentes é, à partida, um sinal de melhoria na segurança. (Cooke e Rohleder, 2006).

A simulação também mostra que pode ser mais produtivo um enfoque na melhoria da cultura de notificação ao remover recriminações do que ao aumentar os incentivos. As recriminações são eficazes como um travão, ao limitar o crescimento das lições aprendidas.

Embora as lições acima sejam o resultado de um modelo baseado na literatura de segurança, elas são igualmente úteis às organizações que desejem utilizar sistemas de aprendizagem de incidentes para melhorar a sua segurança de informação. A abordagem eminentemente técnica na área da segurança de informação acaba por obscurecer os factores humanos, igualmente importantes. Além do mais, os utilizadores dos sistemas são humanos, e, em muitos casos, irão ser os primeiros a detectar incidentes, eventos, ou até os seus sintomas. Os sistemas de aprendizagem de incidentes bem oleados ajudam os utilizadores a aprender factos importantes sobre segurança e porque esta é necessária. Ajuda-os a melhor reconhecer ataques e a aprender como os mitigar.

Os riscos de segurança física podem ser apreendidos como mais reais do que os riscos da segurança de informação. De facto, uma viga de metal que cai pode esmagar-nos, enquanto que um computador que pára é apenas um computador que pára. Pode ser, por isso, mais difícil motivar as pessoas para a segurança da informação, mas esta não é menos importante do que a outra. Mas, e se o computador que pára estiver a controlar uma central nuclear, ou a gerir o tráfego aéreo num movimentado aeroporto?

De facto, nos dias de hoje, com a crescente presença de sistemas informáticos no dia a dia dos cidadãos, que passa pelas actividades lúdicas ou pelo cumprimento de obrigações fiscais ou o estabelecimento de relações financeiras, torna-se evidente a necessidade de garantia de uma boa segurança de informação pelas organizações.

Esta tese permite concluir da grande importância da existência dos sistemas de aprendizagem de incidentes na segurança da informação das organizações.

5.1. Trabalho Futuro

Este estudo foi efectuado com base numa simulação dinâmica, baseando-se em demonstrar que existem muitos desafios, sendo necessário o bom funcionamento dos sistemas de aprendizagem de incidentes.

O modelo apresentado neste estudo é baseado nas boas práticas de segurança, como tal, ele representa a hipótese inicial de como os sistemas de comunicação de incidentes de segurança devem funcionar. A segurança da informação tem alguns desafios que necessitam de ser analisados, como por exemplo, aumentando exponencialmente os volumes de ataque aos sistemas da empresa (Wiik, Gonzalez, e Kossakowski, 2004). Para melhor compreender os desafios específicos que se colocam na segurança da informação, e como trabalho futuro, é necessário um estudo real nas organizações.

Perante estes resultados bastante satisfatórios, foi demonstrado interesse, na implementação de um piloto deste modelo numa área específica, analisando os resultados observados em campo com os obtidos no modelo aqui apresentado, permitindo a evolução do modelo.

6. ANEXOS

Anexo I – Detalhes dos processos CobiT v4.1

PO.01 – Definição do Plano Estratégico de TI (38)

PO.01.1 – Gestão de TI (4)
PO.01.2 – Alinhamento entre as Áreas de Negócio e TI (7)
PO.01.3 – Avaliação da Capacidade e Desempenho Actual (5)
PO.01.4 – Plano Estratégico de TI (8)
PO.01.5 – Planos Tácticos de TI (7)
PO.01.6 – Gestão de Portfólio de TI (7)

PO.02 – Definir o Modelo de Arquitectura de Informação (19)

PO.02.1 – Definir o Modelo de Arquitectura de Informação (3)
PO.02.2 – Manter um Dicionário de Dados e Regras de Sintaxe de Dados (3)
PO.02.3 – Definir e Manter um Esquema de Classificação de Dados (6)
PO.02.4 – Gestão de Integridade da Informação (3)

PO.03 – Definição de Directrizes Tecnológicas (24)

PO.03.1 – Planeamento de Directrizes Tecnológicas (5)
PO.03.2 – Planeamento da Infra-Estrutura Tecnológica (4)
PO.03.3 – Monitorizar as Tendências Futuras e Regulamentação (4)
PO.03.4 – Definir os *Standards* de Tecnologia (7)
PO.03.5 – Comité de Arquitectura de TI (4)

PO.04 – Definição dos Processos, Organização e Relacionamentos de TI (68)

PO.04.1 – Definir a *Framework* de Processos de TI (3)
PO.04.2 – Comité de Estratégia de TI (4)
PO.04.3 – TI *Steering Committee* (6)
PO.04.4 – Inserir a Função de TI na Organização (3)
PO.04.5 – Estrutura Organizacional de TI (2)
PO.04.6 – Definição de Funções e Responsabilidades (9)
PO.04.7 – Responsabilidades pela Garantia de Qualidade de TI (6)
PO.04.8 – Responsabilidades pelo Risco, Segurança e Conformidade (4)
PO.04.9 – Responsabilidade por Sistemas e Dados (3)
PO.04.10 – Supervisão (4)
PO.04.11 – Segregação de Funções (5)
PO.04.12 – *Staffing* de TI(4)
PO.04.13 – Recursos Chave de TI (6)
PO.04.14 – Politicas e Procedimentos para Subcontratação (4)
PO.04.15 – *Relationships* (5)

PO.05 – Gestão do Investimento de TI (32)

PO.05.1 – *Framework* de Gestão Financeira (8)
PO.05.2 – Prioritização no Orçamento de TI (4)
PO.05.3 – Orçamentação de TI (6)
PO.05.4 – Gestão de Custos (8)
PO.05.5 – Gestão de Benefícios (6)

PO.06 – Comunicação dos Objectivos e Directrizes da Gestão (21)

PO.06.1 – Definir Politicas e Ambiente de Controlo de TI (6)
PO.06.2 – *Framework* de Risco e Controlo de TI (3)
PO.06.3 – Gestão de Politicas de TI (5)
PO.06.4 – Politica, Standards e Procedimentos de *Rollout* (4)
PO.06.5 – Comunicação dos Objectivos e Directrizes de TI (3)

PO.07 – Gestão de Recursos Humanos de TI (33)

PO.07.1 – Recrutamento e Retenção de Colaboradores (3)
PO.07.2 – Competências dos Colaboradores (4)
PO.07.3 – Funções de Responsabilidades (4)
PO.07.4 – Formação dos Colaboradores (4)
PO.07.5 – Minimizar a Dependência de Indivíduos (5)
PO.07.6 – Procedimentos de Verificação do Histórico Pessoal/Profissional dos Novos Colaboradores (3)
PO.07.7 – Avaliação de Desempenho do Colaborador (6)
PO.07.8 – Gestão de Transferências e Dispensas (4)

PO.08 – Gestão de Qualidade (23)

PO.08.1 – Sistema de Gestão de Qualidade (6)
PO.08.2 – *Standards* de TI e Práticas de Qualidade (4)
PO.08.3 – *Standards* de Desenvolvimento e Aquisição (3)
PO.08.4 – Focalização no Cliente (4)
PO.08.5 – Melhoria Contínua (3)
PO.08.6 – Medição, Monitorização e Revisão da Qualidade (3)

PO.09 – Resposta ao Risco (22)

PO.09.1 – *Framework* de Gestão de Risco de TI (3)
PO.09.2 – Estabelecer o Contexto do Risco (3)
PO.09.3 – Identificação de Eventos (5)
PO.09.4 – Avaliação do Risco (4)
PO.09.5 – Resposta ao Risco (2)
PO.09.6 – Manutenção e Monitorização de um Plano de Acção do Risco (5)

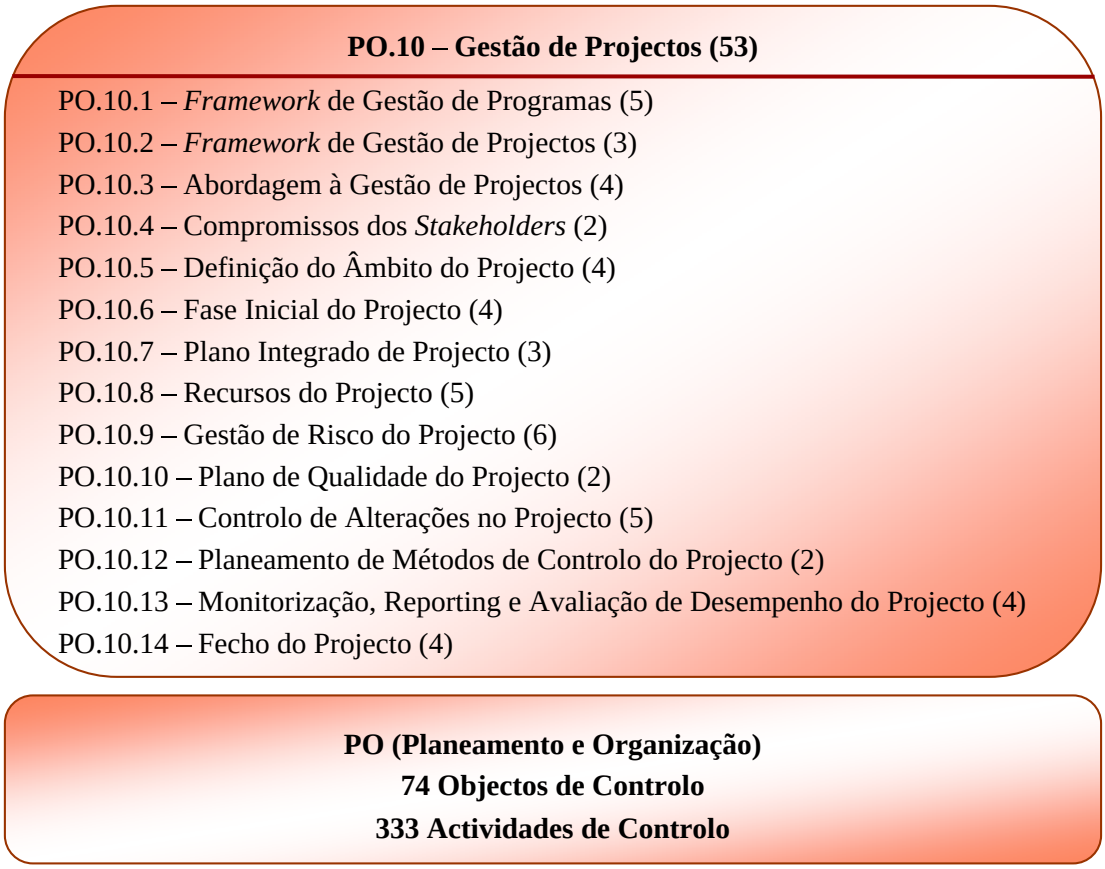


Figura 6.1 – Objectivos de controlo e número de actividade de controlo do domínio Planeamento e Organização (PO)

AI.01 – Identificação de Soluções Tecnológicas (12)

AI.01.1 – Definir e Manter Requisitos Funcionais e Tecnológicos (4)
AI.01.2 – Efectuar e Reportar a Análise de Riscos Associados (3)
AI.01.3 – Estudo da Viabilidade e Formulação de Formas Alternativas de Acção (3)
AI.01.4 – Decidir e Aprovar os Requisitos e Viabilidade (2)

AI.02 – Aquisição e Manutenção de Software Aplicacional (60)

AI.02.1 – Desenho Alto-Nível (6)
AI.02.2 – Desenho Detalhado (11)
AI.02.3 – Controlo da Aplicação e Auditoria (5)
AI.02.4 – Segurança e Disponibilidade da Aplicação (5)
AI.02.5 – Configuração e Implementação da Aplicação Adquirida (11)
AI.02.6 – Actualizações Principais dos Sistemas Existentes (2)
AI.02.7 – Desenvolvimento de Software Aplicacional (8)
AI.02.8 – Garantia de Qualidade do Software (4)
AI.02.9 – Gestão de Requisitos Aplicacionais (3)
AI.02.10 – Manutenção de Software Aplicacional (5)

AI.03 – Aquisição e Manutenção da Infra-Estrutura Tecnológica (20)

AI.03.1 – Plano de Aquisição de Infra-Estrutura Tecnológica (4)
AI.03.2 – Protecção e Disponibilidade de Recursos da Infra-Estrutura (9)
AI.03.3 – Manutenção de Infra-Estruturas (5)
AI.03.4 – Ambiente de Testes de Viabilidade (2)

AI.04 – Suporte à Operação e Utilização (18)

AI.04.1 – Planeamento de Soluções Operacionais (2)
AI.04.2 – Transferência de Conhecimentos para a Gestão do Negócio (5)
AI.04.3 – Transferência de Conhecimento para os Utilizadores Finais (6)
AI.04.4 – Transferência de Conhecimento para Pessoal Operacional e de Suporte (5)

AI.05 – Contratação de Recursos de TI (19)

AI.05.1 – Controlo das Contratações (4)
AI.05.2 – Gestão de Contratos com Fornecedores (6)
AI.05.3 – Selecção de Fornecedores (6)
AI.05.4 – Aquisição de Recursos de TI (3)

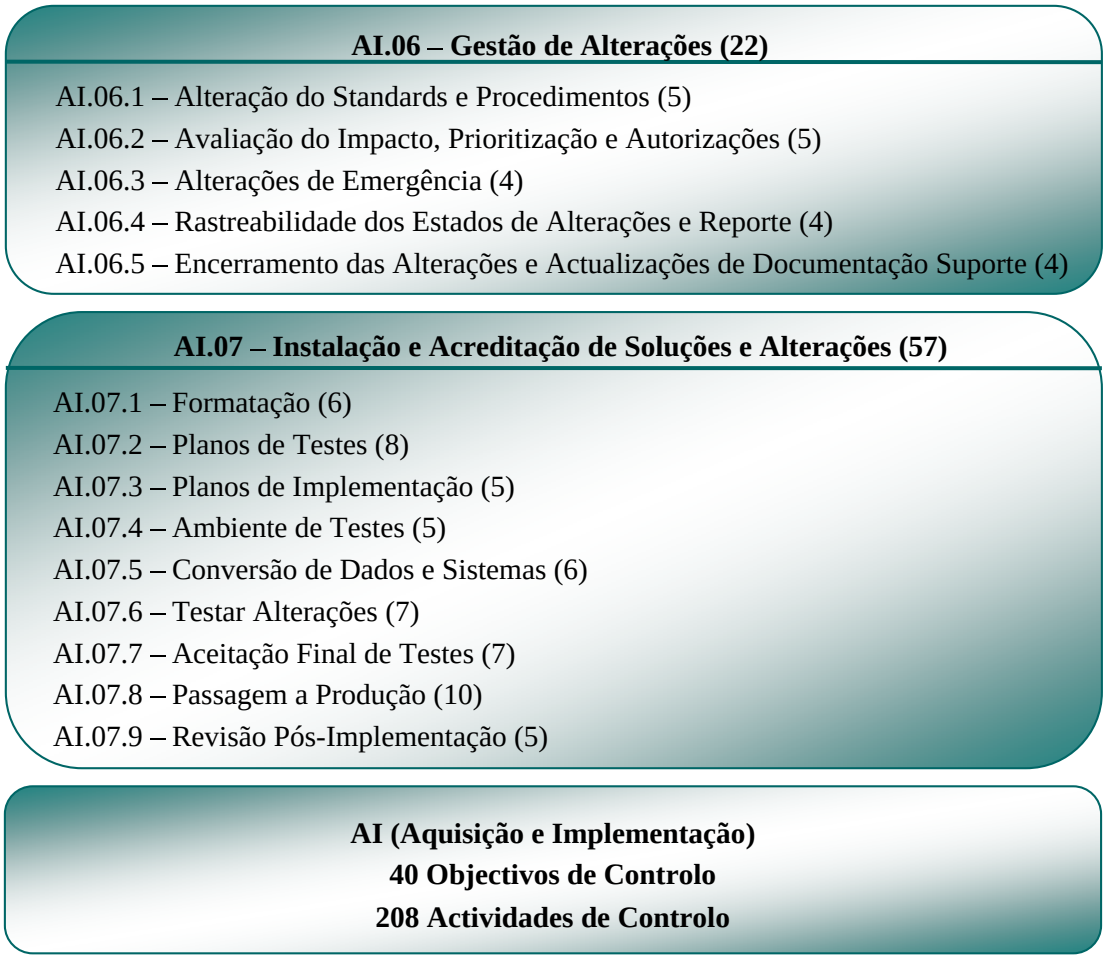


Figura 6.2 – Objectivos de controlo e número de actividades de controlo do domínio Aquisição e Implementação (AI)

DS.01 – Definição da Gestão de Níveis de Serviço (19)

DS.01.1 – *Framework* de Gestão de Níveis de Serviço (6)
DS.01.2 – Definição de Serviços (2)
DS.01.3 – Acordos de Nível de Serviço (4)
DS.01.4 – Acordos de Nível Operacional (2)
DS.01.5 – Monitorização e Reporte dos Níveis de Serviço Atingidos (3)
DS.01.6 – Revisão de Acordos e Contratos de Níveis de Serviço (2)

DS.02 – Gerir Serviços de Entidades Externas (19)

DS.02.1 – Identificação dos Relacionamentos com Todos os Fornecedores (2)
DS.02.2 – Gestão de Relação com Fornecedores Externos (8)
DS.02.3 – Gestão de Risco de Fornecedores Externos (4)
DS.02.4 – Monitorização de Desempenho dos Fornecedores Externos (5)

DS.03 – Gestão de Desempenho e Capacidade (19)

DS.03.1 – Planeamento do Desempenho e Capacidade (3)
DS.03.2 – Desempenho e Capacidade Actual (3)
DS.03.3 – Desempenho e Capacidade Futura (4)
DS.03.4 – Disponibilidade e Recursos de TI (5)
DS.03.5 – Monitorização e Reporte (4)

DS.04 – Garantia de Continuidade do Serviço (38)

DS.04.1 – Estabelecer a *Framework* para a Continuidade (3)
DS.04.2 – Planos de Continuidade (8)
DS.04.3 – Recursos Críticos de TI (2)
DS.04.4 – Manutenção dos Planos de Continuidade de TI (3)
DS.04.5 – Testar o Plano de Continuidade de TI (6)
DS.04.6 – Formação no Plano de Continuidade de TI (4)
DS.04.7 – Distribuição do Plano de Continuidade de TI (3)
DS.04.8 – Recuperação e Recomeço dos Serviços (2)
DS.04.9 – Armazenamento de Cópias de Segurança de Dados em Centros Alternativos (6)
DS.04.10 – Revisão Após Retorno à Normal Operacionalidade de TI (1)

DS.05 – Gestão da Segurança de TI (46)

DS.05.1 – Gerir a Segurança de TI (4)
DS.05.2 – Plano de Segurança de TI (5)
DS.05.3 – Gestão de Identidades (IDs) (5)
DS.05.4 – Gestão de Contas de Utilizador (2)
DS.05.5 – Testes de Segurança, Vigilância e Monitorização (2)
DS.05.6 – Definição de Incidentes de Segurança (3)
DS.05.7 – Protecção da Segurança Tecnológica (4)
DS.05.8 – Gestão de Chaves Criptográficas (7)
DS.05.9 – Prevenção, Detecção e Correcção de Software Malicioso (5)
DS.05.10 – Segurança de Redes (6)
DS.05.11 – Troca de Dados Sensíveis (3)

DS.06 – Identificação e Imputação de Custos (16)

DS.06.1 – Definição dos Serviços (3)
DS.06.2 – Contabilidade de TI (5)
DS.06.3 – Modelo de Imputação de Custos e Facturação (5)
DS.06.4 – Manutenção do Modelo de Imputação de Custos (3)

DS.07 – Formação e Treino de Utilizadores (12)

DS.07.1 – Identificar de Necessidade de Formação (4)
DS.07.2 – Formação e Treino de Utilizadores (3)
DS.07.3 – Avaliação da Formação Recebida (5)

DS.08 – Gestão do *Service Desk* e Incidentes (21)

DS.08.1 – Apoio ao Utilizador (*Service Desk*) (5)
DS.08.2 – Registar os Pedidos dos Utilizadores (6)
DS.08.3 – Escalar os Incidentes (4)
DS.08.4 – Fechar Incidentes (4)
DS.08.5 – Reportar e Analisar Tendências (4)

DS.09 – Gestão de Configurações (17)

DS.09.1 – Repositório de Configurações e *Baseline* (6)
DS.09.2 – Identificação e Manutenção de Itens de Configuração (8)
DS.09.3 – Revisão da Integridade dos Dados de Configuração (3)

DS.10 – Gestão de Problemas (18)

DS.10.1 – Identificação e Classificação de Problemas (5)
DS.10.2 – Acompanhamento e Resolução de Problemas (7)
DS.10.3 – Encerramento de Problemas (2)
DS.10.4 – Integração da Gestão de Configurações, Incidentes e Problemas (4)

DS.11 – Gestão de Dados (41)

DS.11.1 – Requisitos do Negócio para a Gestão de Dados (9)
DS.11.2 – Acordos de *Storage* e Retenção (7)
DS.11.3 – Sistemas de Gestão da Biblioteca de Media (4)
DS.11.4 – Destruição (6)
DS.11.5 – *Backup* e Recuperação (9)
DS.11.6 – Requisitos de Segurança para a Gestão de Dados (6)

DS.12 – Gestão de Instalações Físicas (40)

DS.12.1 – Selecção do Local e do *Layout* (3)
DS.12.2 – Medidas de Segurança Física (11)
DS.12.3 – Gestão dos Acessos Físicos (7)
DS.12.4 – Protecção Contra Factores Ambientais (8)
DS.12.5 – Gestão das Instalações Físicas (11)

DS.13 – Gestão de Operações (26)

DS.13.1 – Instruções e Procedimentos de Operação (5)
DS.13.2 – Agendamento de Tarefas (4)
DS.13.3 – Monitorização de Infra-Estruturas de TI (6)
DS.13.4 – Protecção da Documentação e Dispositivos de *Outputs* Sensíveis (5)
DS.13.5 – Manutenção Preventiva para *Hardware* (6)

DS (Entrega e Suporte)
67 Objectivos de Controlo
334 Actividades de Controlo

Figura 6.3 – Objectivos de controlo e número de actividades de controlo do domínio Entrega e Suporte (DS)

ME.01 – Monitorização e Avaliação do Desempenho de TI (30)

ME.01.1 – Definir a Abordagem de Monitorização (7)
ME.01.2 – Definir e Recolher Informação para Monitorização (5)
ME.01.3 – Gerir o Processo de Monitorização (5)
ME.01.4 – Avaliação do Desempenho (5)
ME.01.5 – Reportar Indicadores para a Gestão (3)
ME.01.6 – Acções de Remediação (5)

ME.02 – Monitorização e Avaliação do Controlo Interno (35)

ME.02.1 – Monitorização da *Framework* de Controlo Interno (6)
ME.02.2 – Rever e Supervisionar os Controlos Internos (5)
ME.02.3 – Controlo de Excepções (5)
ME.02.4 – Controlo de Auto-avaliação (6)
ME.02.5 – Garantia de Controlo Interno (4)
ME.02.6 – Controlo Interno de Terceiros (3)
ME.02.7 – Acções de Remediação (6)

ME.03 – Garantia de Conformidade com os Requisitos Externos (19)

ME.03.1 – Identificação dos Requisitos de Conformidade Legais, Regulatórios e Contratuais (5)
ME.03.2 – Optimização da Resposta aos Requisitos Externos (4)
ME.03.3 – Avaliação da Conformidade com os Requisitos Externos (3)
ME.03.4 – Garantia de Conformidade pela Positiva (5)
ME.03.5 – Reporte Integrado (2)

ME.04 – Governação de TI (31)

ME.04.1 – Implementar *Framework* de Governo das TI (6)
ME.04.2 – Alinhamento estratégico (3)
ME.04.3 – Entrega de Valor (6)
ME.04.4 – Gestão de Recursos (4)
ME.04.5 – Gestão do Desempenho (3)
ME.04.6 – Auditoria Independente (3)

ME (Monitorização e Avaliação)
23 Objectivos de Controlo
115 Actividades de Controlo

Figura 6.4 – Objectivos de controlo e número de actividades de controlo do domínio Monitorização e Avaliação (ME)

Anexo II – Estrutura do modelo CobiT

O modelo *CobiT* une os requisitos de negócio para informação e governação aos objectivos da função de serviços de TI. O modelo de processos do *CobiT* permite que as actividades de TI e os recursos que as suportam sejam apropriadamente geridos e controlados com base nos objectivos de controle, bem como alinhados e monitorizados usando os objectivos e métricas do *CobiT*, conforme ilustrado na **Figura 6.5** pelo cubo do *CobiT*.

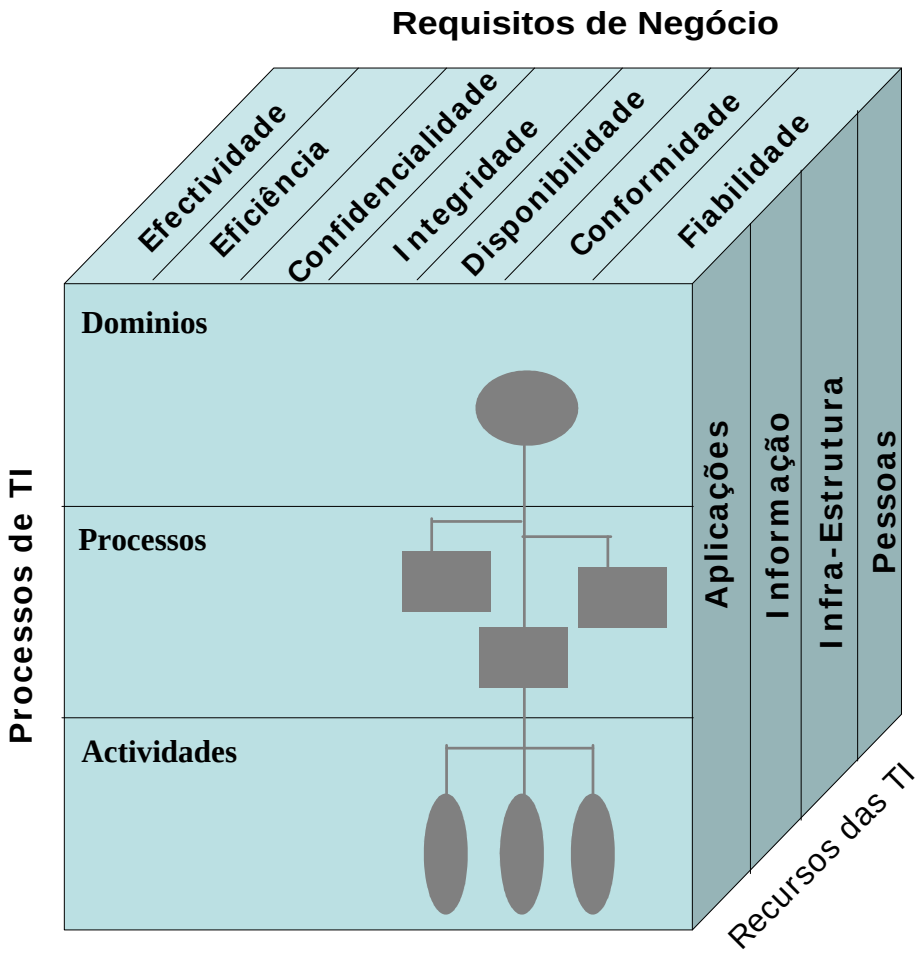


Figura 6.5 - Cubo do CobiT *(CobiT 4.1 Framework)*

Anexo III - SGSI - Sistemas de Gestão da Segurança da Informação

O processo de um SGSI deve:

- Partir de uma decisão estratégica da organização;
- Ser adaptado ás necessidades e objectivos específicos de cada negócio;
- Ser actualizado regularmente;
- Usar o ciclo PDCA – *Plan, Do, Check, Act*.

O modelo de implementação de um SGSI segue o ciclo PDCA, tal como indicado abaixo.

Figura 6.6 - Modelo "Plan-Do-Check-Act"

Anexo IV – Fluxos da Gestão de Incidentes

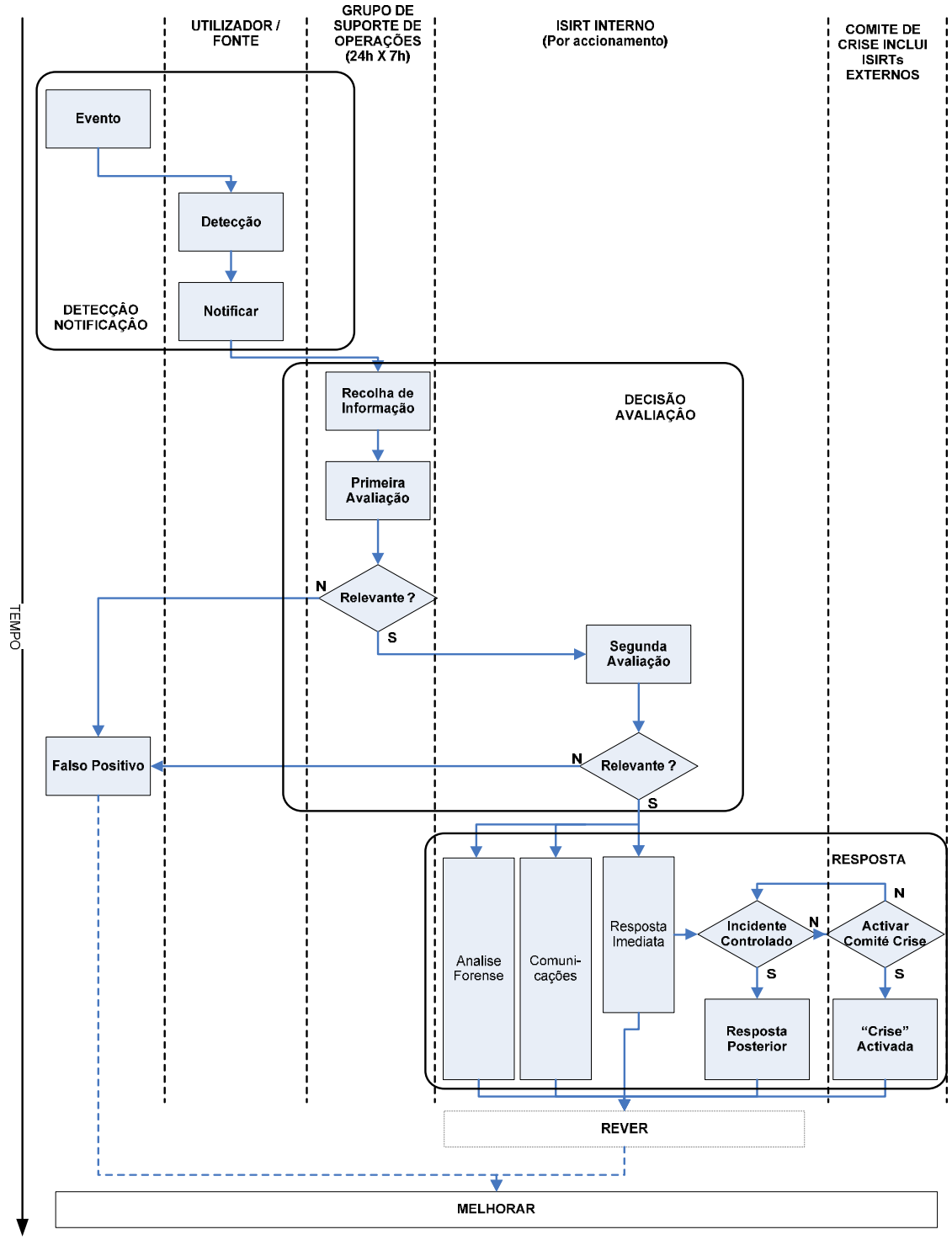


Figura 6.7 – Fluxos da Gestão de Incidentes na Segurança da Informação (ISO,2005)

Anexo V – Modelo de Gestão de Incidentes

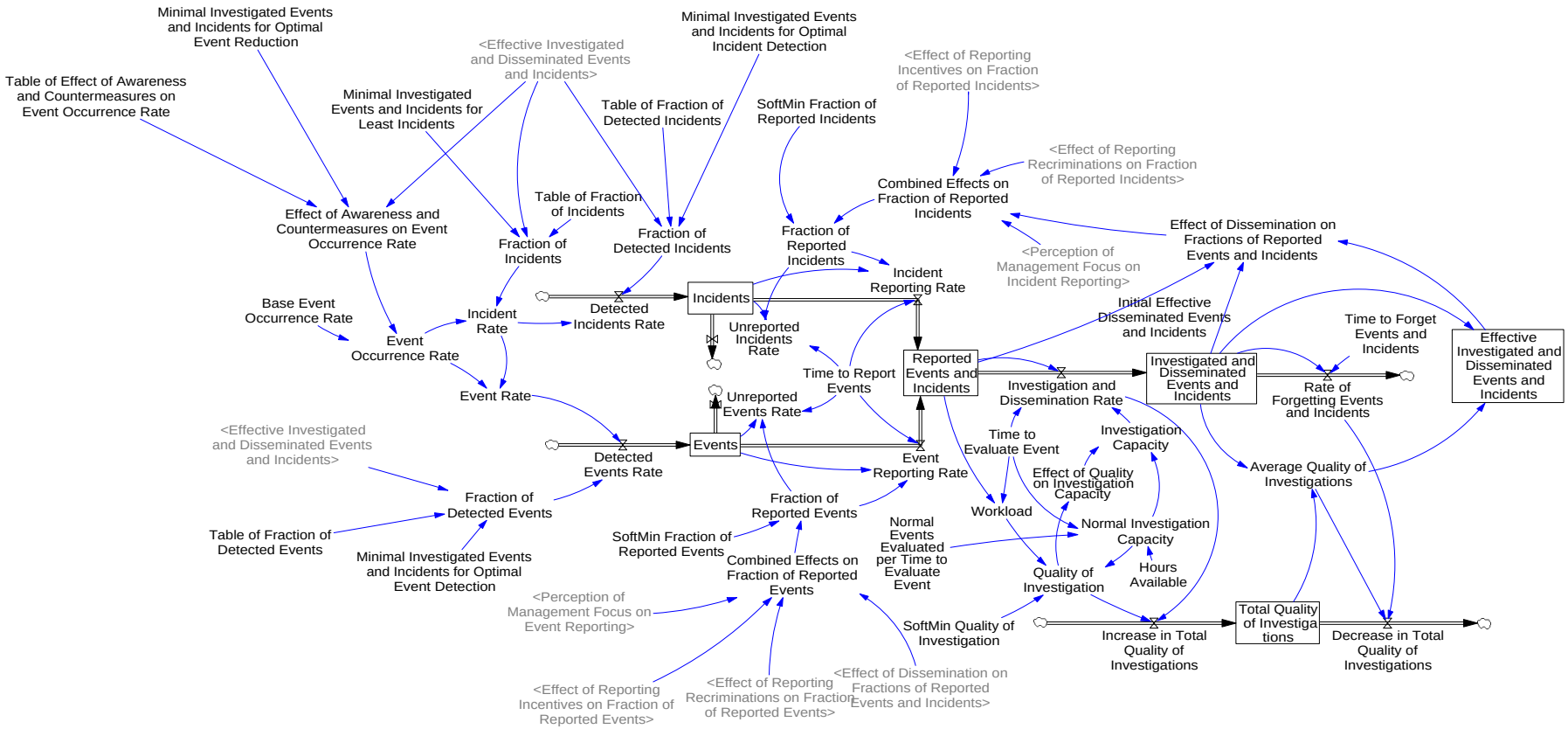


Figura 6.8 – Detalhe do Modelo de Gestão de Incidentes (Adaptado Sveen, 2010)

Anexo VI – Principais Fórmulas e Indicadores

Constante Exógena:

Base Event Occurrence Rate = 427 events / month

Incidentes e Eventos:

Event Occurrence Rate = Base Event Occurrence Rate * Effect of Awareness and Countermeasures on Event Occurrence Rate

Undetected Incidents Rate = Event Occurrence Rate * Fraction of Incidents

Undetected Events Rate = Event Occurrence Rate - Undetected Incidents

Detected Incidents Rate = Incident Rate * Fraction of Detected Incidents

Detected Events Rate = Event Rate * Fraction of Detected Events

Incident Reporting Rate = (Incidents * Fraction of Reported Incidents) / Time to Report Events

Unreported Incidents Rate = (Incidents*(1-Fraction of Reported Incidents))/Time to Report Events

Event Reporting Rate = (Events * Fraction of Reported Events) / Time to Report Events

Unreported Events Rate = (Events * (1-Fraction of Reported Events)) / Time to Report Events

Investigation and Dissemination Rate = min(Investigation Capacity, Reported Events and Incidents/Time to Evaluate Event)

Qualidade da Investigação:

Workload = Reported Events and Incidents/Time to Evaluate Event

Quality of Investigation = (Normal Investigation Capacity/Workload)*SoftMin Quality of Investigation(1/(Normal Investigation Capacity/Workload))

Investigation Capacity = Normal Investigation Capacity*Effect of Quality on Investigation Capacity

Total Quality of Investigations (stock) = +Increase in Total Quality of Investigations-Decrease in Total Quality of Investigations

Average Quality of Investigations = Total Quality of Investigations/Investigated and Disseminated Events and Incidents

Effective Investigated and Disseminated Events and Incidents = Investigated and Disseminated Events and Incidents*Average Quality of Investigations

Motivação para Reportar Incidentes:

Fraction of Reported Incidents = Combined Effects on Fraction of Reported Incidents*SoftMin Fraction of Reported Incidents(1/Combined Effects on Fraction of Reported Incidents)

Combined Effects on Fraction of Reported Incidents = Effect of Dissemination on Fractions of Reported Events and Incidents*Effect of Reporting Incentives on Fraction of Reported Incidents * Effect of Reporting Recriminations on Fraction of Reported Incidents*Perception of Management Focus on Incidents

Fraction of Reported Events = Combined Effects on Fraction of Reported Events * SoftMin Fraction of Reported Events (1/Combined Effects on Fraction of Reported Events)

Combined Effects on Fraction of Reported Events = Effect of Dissemination on Fractions of Reported Events and Incidents * Effect of Reporting Incentives on Fraction of Reported Events * Effect of Reporting Recriminations on Fraction of Reported Events * Perception of Management Focus on Events

Focus da Gestão:

Perception of Management Focus on Incident Reporting = Integ(Change of Perception of Management Focus on Incidents)

Change in Perception of Management Focus on Incident Reporting = (Management Focus on Incidents-Perception of Management Focus on Incident Reporting) / Time to Change Perception of Management Focus

Perception of Management Focus on Event Reporting = Integ(Change of Perception of Management Focus on Event Reporting)

Change of Perception of Management Focus on Event Reporting = (Management Focus on Events - Perception of Management Focus on Event Reporting) / Time to Change Perception of Management Focus

Recriminações por notificar:

Rate of Increase in Reporting Recriminations = (Event Reporting Rate+Incident Reporting Rate)*Effectiveness of Recriminations

Rate of Forgetting Reporting Recriminations = Reporting Recriminations / Time to Forget Reporting Recriminations

Effect of Reporting Recriminations on Fraction of Reported Incidents = Table of Effect of Reporting Recriminations on Fraction of Reported Incidents (Reporting Recriminations / Minimal Recriminations for Worst Performance)

Effect of Reporting Recriminations on Fraction of Reported Events = Table of Effect of Reporting Recriminations on Fraction of Reported Events (Reporting Recriminations / Minimal Recriminations for Worst Performance)

Incentivos à notificação:

Rate of Increase in Reporting Incentives = (Event Reporting Rate+Incident Reporting Rate)*Effectiveness of Incentives

Rate of Forgetting Reporting Incentives = Reporting Incentives / Time to Forget Reporting Incentives

Effect of Reporting Incentives on Fraction of Reported Incidents = Table of Effect of Reporting Incentives on Fraction of Reported Incidents (Reporting Incentives / Normal Reporting Incentives)

Effect of Reporting Incentives on Fraction of Reported Events = Table of Effect of Reporting Incentives on Fraction of Reported Events (Reporting Incentives / Normal Reporting Incentives)

Efeitos da aprendizagem:

Effect of Dissemination on Fractions of Reported Events and Incidents = Effective Investigated and Disseminated Events and Incidents / (Investigated and Disseminated Events and Incidents + Reported Events and Incidents)

Effect of Awareness and Countermeasures on Event Occurrence Rate = Table of Effect of Awareness and Countermeasures on Event Occurrence Rate (Effective Investigated and Disseminated Events and Incidents / Minimal Investigated Events and Incidents for Optimal Performance)

Fraction of Incidents = Table of Fraction of Incidents (Effective Investigated and Disseminated Events and Incidents / Minimal Investigated Events and Incidents for Optimal Performance)

Fraction of Detected Incidents = Table of Fraction of Detected Incidents (Effective Investigated and Disseminated Events and Incidents / Minimal Investigated Events and Incidents for Optimal Performance)

Fraction of Detected Events = Table of Fraction of Detected Events (Effective Investigated and Disseminated Events and Incidents / Minimal Investigated Events and Incidents for Optimal Event Detection and Reporting Performance)

7. GLOSSÁRIO

Ameaça – Um evento que pode explorar uma vulnerabilidade e expor uma organização a um risco.

Anomalia Grave - Situação de perturbação grave de um serviço ou função, cujas consequências – reais ou potenciais - sejam de tal modo relevantes e originem prejuízos significativos, seja materiais, sejam de imagem, que frequentemente não se esgotam no momento da sua resolução. Tendencialmente e tipicamente, este tipo de situações, suscitam a necessidade de justificação através de relatórios formais para a Administração das empresas. É um incidente cujas características por vezes justificam o seu tratamento como problema.

Amostra – É uma selecção de elementos representativos de uma população.

Alteração - Qualquer acréscimo, modificação ou eliminação de alguma componente dos Sistemas de Informação (SI), passível de afectar os respectivos Níveis de Serviço e, consequentemente, susceptível de provocar reclamações de utilizadores ou clientes. De entre as componentes dos SI consideradas incluem-se hardware, software base, software de produtos, software aplicacional, comunicações, documentação ou infra-estruturas gerais de apoio (por exemplo: energia, cablagens, etc.).

Análise de risco – Análise das ameaças, impactos e vulnerabilidades da informação, das facilidades de processamento da informação e da probabilidade da sua ocorrência.

***Benchmarking* –** Técnica ou processo sistemático de comparação de resultados e processos organizacionais entre duas ou mais organizações. O objectivo é que, através da aprendizagem sobre melhores práticas, estas sejam aplicadas e alcançados os mesmos níveis de desempenho ou superiores; Comparação de uma referência com uma linha de base ou com uma melhor prática. O termo comparativo também significa a criação de uma série de referências com o passar do tempo e comparar os resultados para medir o progresso ou melhoria.

***Brainstorming* ou "tempestade de ideias" –** É uma actividade desenvolvida para explorar a potencialidade criativa de um indivíduo ou de um grupo, colocando-a ao serviço de objectivos pré-determinados.

***Business Case* –** Justificação de um projecto, apresentado em termos de benefícios, custos tangíveis e da viabilidade técnica e organizacional do projecto proposto.

Ciclo PDCA (Plan, Do, Check, Act)– É um ciclo de desenvolvimento constituído por quatro etapas aplicadas à gestão de um processo (Planear, Executar, Verificar e Actuar). Tem o foco na melhoria contínua.

Controlo – É uma forma de gerir um risco, garantindo que um objectivo de negócio é atingido, ou que um processo seja seguido. É a medida posta em prática para regular, orientar e monitorizar um risco.

Desenho do controlo – Controlo definido para atingir o objectivo de controlo.

Domínio de Impacto - Extensão dos efeitos da ocorrência do incidente, ou seja, quantidade de utilizadores/clientes afectados pela interrupção ou degradação do serviço.

Evento – Uma ocorrência / facto / acção ou processo observável.

Impacto – Medida relativa ao efeito de um evento nas tarefas, actividades, processos e serviços de uma organização.

Incidente - Incidente é qualquer evento que possa causar uma interrupção de um serviço de TI ou a redução da sua qualidade.

***Knowledge Base* de Soluções** - Base de dados de soluções ou *workarounds* definidos, para aplicação na resolução de incidentes tipificados.

Matriz de Atribuição de Responsabilidades (RACI *tables*) – Modelo desenvolvido para ajudar a definir funções e responsabilidades, atribuindo quem é Responsável (*Responsible*), Autoridade (*Accountable*), Consultado (*Consulted*) e Informado (*Informed*).

Maturidade – Nível de confiança, eficácia e eficiência de um processo, actividade, função, organização, entre outros. Um processo com um maior nível de maturidade está mais alinhado com os objectivos e estratégia da organização e é suportado por uma estrutura de melhoria contínua.

Melhores práticas – Utilização de métodos ou iniciativas que conduzem a organização a um bom desempenho, baseando-se na adocção de práticas de gestão inovadoras ou interessantes, as quais foram identificadas através, por exemplo, do *benchmarking*.

Melhoria continua – Técnica de mudança organizacional, que envolve toda a organização (colaboradores e gestores) no esforço de melhoria dos processos de trabalho tendo em vista a qualidade dos serviços, a economia de recursos e de tempo.

Métrica – Medida quantitativa resultante de uma medição, a qual suporta o cálculo de indicadores.

Monitorização – Conjunto de tarefas orientadas à intercepção de eventos e detecção/registo de incidentes ou ocorrências, podendo usar-se para o efeito ferramentas e procedimentos específicos executados numa base periódica e sistemática.

Não Conformidade – A não satisfação de um ou vários requisitos.

Norma – Conjunto de regras estabelecidas pela organização para serem cumpridas na execução de um processo, de uma actividade ou de uma tarefa.

Objectivo – É um fim desejado, que é considerado chave para a organização e que reflecte a sua visão. Cada objectivo é medido com base em indicadores, relativamente aos quais se estabelecem metas a atingir. Os objectivos têm responsáveis que devem acompanhar o seu cumprimento.

Objectivo de controlo – A afirmação de um resultado desejado ou proposto para ser atingido, através da implementação de procedimentos de controlo num determinado processo.

Ocorrência de Indisponibilidade de Serviço - Formalização de uma situação, real ou alegada, de degradação grave ou indisponibilidade de Serviço desde que se verifique dentro, total ou parcialmente, do Período Acordado de Serviço (PAS).

Pedido de Alteração - Cada alteração é formalizada na ferramenta de suporte através de um registo electrónico único designado por Pedido de Alteração ou *Request For Change* (RFC).

Período Acordado de Serviço - É o período de disponibilidade de Serviço acordado com o Cliente ou no qual se reconhece que o Serviço deve estar impreterivelmente disponível.

Política – É a combinação entre um objectivo e os meios para a sua prossecução. Representa as intenções e expectativas da Gestão, documentadas formalmente.

Problema - Situação especialmente crítica ou de diagnóstico complexo e que pode decorrer tanto de um Incidente como de uma Ocorrência de Indisponibilidade de Serviço. É a causa desconhecida de um ou mais incidentes (não necessariamente resolvida no momento em que o incidente é fechado).

Procedimento – É a documentação das tarefas necessárias para a execução de actividades associadas a processos.

Processo – Conjunto de actividades inter-relacionadas e inter-actuantes que transformam entradas (inputs) em saídas (outputs).

Processo Gestão de Alterações - Tem por objectivo definir mecanismos que permitam a gestão, o controlo e a monitorização de todos os pedidos de alterações, de uma forma estruturada, com vista a: i) maximizar o tratamento eficaz de todas as Alterações, por forma

a minimizar o impacto nos serviços prestados ao cliente causados por incidentes resultantes dessas Alterações; ii) manter o equilíbrio adequado entre a necessidade da Alteração e o potencial impacto negativo resultante da mesma; iii) garantir a máxima eficiência e eficácia na implementação das Alterações; iv) garantir a máxima eficiência das Alterações implementadas.

Processo Gestão de Clientes - Tem por objectivo definir a interface entre o prestador do serviço e os Clientes, a qual permita: i) receber e responder aos pedidos dos clientes segundo os critérios definidos; ii) preparar e submeter propostas de solução; iii) negociar, estabelecer e acompanhar acordos estabelecidos com o Cliente.

Processo Gestão de Configurações - Visa manter a informação centralizada sobre todos os elementos que constituem a infra-estrutura de SI/TI, permitindo o controlo eficaz das suas alterações, bem como a sua verificação de forma a garantir a correcção da informação da configuração face à realidade e à conformidade com requisitos específicos.

Processo Gestão da Indisponibilidade - Tem por objectivos: i) garantir que todas as reclamações, incidentes, problemas, alterações ou outros eventos, caso provoquem indisponibilidade, conduzem ao registo da respectiva ocorrência de indisponibilidade e ao consequente tratamento/acompanhamento até ao seu fecho; ii) garantir o registo consistente dos dados necessários para uma correcta medição dos níveis de disponibilidade; iii) permitir a obtenção de indicadores sobre as indisponibilidades existentes por forma a apoiar a identificação de pontos de melhoria do(s) serviço(s) e identificação de causas de indisponibilidades recorrentes; iv) melhorar a eficiência na resposta a situações de indisponibilidade de serviços; v) garantir a comunicação atempada e coerente da informação relativa a indisponibilidades de serviços às áreas com contacto com os clientes/utilizadores, por forma a diminuir o impacto da imagem do serviço junto dos clientes/utilizadores.

Processo Gestão de Problemas - Tem como objectivos minimizar os impactos negativos no negócio causados por incidentes resultantes de problemas ou erros na infra-estrutura de TI e prevenir a recorrência de incidentes relacionados com esses problemas. Incentiva a investigação da origem dos incidentes e a execução de acções para melhorar ou corrigir essas situações. Consiste num conjunto de actividades designadas por Controlo de Problemas, Controlo de Erros, Reporting e Gestão do Conhecimento, Gestão Proactiva de Problemas e Gestão de Crises.

Processo Gestão do Risco - Processo sistemático e organizado de tomada de decisão, que identifica, analisa, planeia, monitoriza, controla, comunica e regista riscos (ameaças ou oportunidades), de uma forma eficiente, com o objectivo de colocar o risco associado à

actividade da empresa abaixo de níveis considerados aceitáveis pela mesma. A gestão de riscos está associada tipicamente à prevenção de eventos indesejáveis, mas deve incluir também a promoção de eventos positivos (oportunidades). O Processo tem duas vertentes de aplicação: i) gestão de risco de projectos, visando fundamentalmente gerir eventos de risco de forma a aumentar a probabilidade de sucesso dos projectos; ii) gestão de risco operacional e tecnológico, visando gerir os eventos de risco de impacto negativo que possam ocorrer nas componentes de infra-estruturas, hardware, software, comunicações, segurança e nas componentes humana, processual ou logística que os suportam.

Processo Manutenção - Tem por objectivo garantir que as necessidades do cliente do sistema/aplicação continuam a ser asseguradas, que o produto (sistema, software, etc.) ou serviço, após a sua entrega para exploração/utilização, continua a desempenhar a sua função. Inclui actividades de correcção de erros, melhoria de performance ou de outros atributos e, ainda, actividades de adaptação a alterações que ocorram na sua envolvente e que ponham em causa as funcionalidades disponíveis. Pretende-se, também, que a modificação, a restauração e/ou a eliminação de um produto ou serviço seja efectuada preservando a integridade da operação do negócio.

Reposição de Serviço - Retoma de um serviço de TI pelos utilizadores depois da resolução e recuperação após incidente.

Requisito – Desenho de um serviço que é pretendido. Expressão no conteúdo de um documento resumindo critérios a serem satisfeitos se se pretender reclamar a conformidade com o documento e em relação aos quais não são permitidos desvios.

Segurança da informação – Protecção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detectar, documentar e contrariar tais ameaças.

SOA (*Statement of Applicability*) – A declaração de aplicabilidade é um documento que identifica os controlos escolhidos para o ambiente de controlo e explica como e porque é que eles são apropriados. O SOA resulta de uma avaliação do risco e no caso de se pretender a conformidade com a norma ISO27001, tem que relacionar directamente os controlos seleccionados com os riscos que eles pretendem mitigar. O SOA também deve indicar os controlos excluídos e a razão da exclusão.

Solução definitiva - Identificação de uma alteração ou conjunto de alterações que permite a eliminação estrutural e definitiva de um erro. Após a aplicação com sucesso de uma solução, não voltarão a ocorrer incidentes causados por esse erro.

Sponsor ou **Patrocinador –** É quem dirige, justifica, facilita e apoia o projecto ou outro empreendimento. É também responsável pela realização dos objectivos de negócio que o projecto ou empreendimento suportam. É responsável pelos benefícios do projecto, por aceitar os resultados e deve ser elemento do *Steering Committee*, caso este exista.

Stakeholders **ou Partes Interessadas –** Pessoa ou organização activamente envolvidos num projecto/empreendimento ou cujos interesses possam ser positivamente ou negativamente afectados pela sua execução ou conclusão.

Steering Committee **–** Contribui para os resultados da Organização fornecendo orientação sénior. O *Steering Committee* toma decisões executivas, resolve problemas e conflitos que não podem ser tratados a um nível mais baixo.

Tecnologias de Informação (TI) – Tecnologias necessárias para o processamento da informação ou, mais especificamente, a utilização de *hardware* e *software* para converter, armazenar, proteger, tratar, transmitir e recuperar a informação, a partir de qualquer lugar e em qualquer momento.

Workaround **-** É uma solução temporária para um incidente ou problema que permite evitá-lo ou ultrapassá-lo (eliminando ou reduzindo os seus efeitos).

8. REFERÊNCIAS

- Anderson, R. (Ed.) (2001). Why information security is hard—an economic perspective. 17th Annual Computer Security Applications Conference, 2001 (ACSAC 2001); 10–14 December.
- Anderson, D. J., & Webster, C. S. (2001). A system approach to the reduction of medication error on the hospital ward. Journal of Advanced Nursing, 35(1), 34–41.
- Basel Committee on Banking Supervision – Bank for International Settlements (2010). Principles for enhancing corporate governance.
- Barlas, Y. (1989). Multiple tests for validation of system dynamics type of simulation models. European Journal of Operations Research, 42, 59–87.
- Barlas, Y. (1996). Formal aspects of model validity and validation in system dynamics. System Dynamics Review, 12(3), 183–210.
- Bhatt, G. D. (2001). Knowledge management in organizations: Examining the interaction between technologies, techniques, and people. Journal of Knowledge Management, 5(1), 68–75.
- Carlson, T. (2008).Understanding ISO 27001,Orange Parachute Inc..
- Campbell, S. (2006).How to think about security failures. Communications of the ACM, 49(1), 37–39 (01).
- CERT.PT em WWW.CERT.PT, visto em 2010/09/15.
- Cooke, D. L., & Rohleder, T. R. (2006). Learning from incidents: From normal accidents to high reliability. System Dynamics Review, 22(3), 213–239.
- Damodaran, L., & Olphert, W. (2000). Barriers and facilitators to the use of knowledge management systems. Behaviour & Information Technology, 19(6), 405 –413.
- Davenport, T. H. (1997). Information ecology: Mastering the information and knowledge environment. New York: Harvard Business School Press.
- Davenport, T. H., & Prusak, L. (1998). Working knowledge: How organizations manage what they know. Boston: Harvard Business School Press.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
- Debar, H., & Viinikka, J. (2005). Intrusion detection: Introduction to intrusion detection and security information management. In A. Aldini, R. Gorrieri, & F. Martinelli (Eds.), Foundations of security analysis and design III (pp. 207–236). Heidelberg: Springer Berlin.
- Debowski, S. (2006). Knowledge management. Australia: John Wiley & Sons.
- Forrester, J. W. (1961). Industrial dynamics. Cambridge MA: Productivity Press.
- Forrester, J. W. (1994). Policies, decisions, and information sources for modeling. In J. D. W. Morecroft, J. D. Sterman (Eds.), Modeling for learning organizations (pp. 51–84). Portland, OR: Productivity Press.
- Forrester, J. W., & Senge, P. M. (1981). Tests for building confidence in system dynamics models. TIMS Studies in the Management Sciences, 14, 209–228.

- Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. Information Systems Research, 16(2), 186–208.
- Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: An organizational capabilities perspective. Journal of Management Information Systems, 18(1), 185–214.
- Gonzalez, J. J. (2005). Towards a cyber security reporting system—a quality improvement process. In B. A. G. Rune Winther, & G. Dahll (Eds.), Computer safety, reliability, and security. Heidelberg: Springer.
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438–457 (November).
- Gordon, L. A., Loeb, M., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. Journal of Accounting Public Policy, 22(6), 461–485.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). CSI/FBI Computer Crime and Security Survey. Technical Report: Computer Security Institute.
- Görling, S. (2006). The myth of user education. Virus Bulletin Conference; 2006 11–13 October; Montréal, Canada.
- Halal, G. (1998). The infinite resource. San Francisco: Jossey-Bass Publishers.
- Haley, C. B., Moffett, J. D., Laney, R., & Nuseibeh, B. (Eds.) (2005). A framework for security requirements engineering. The 2006 International Workshop on Software Engineering for Secure Systems; Shanghai, China IEEE.
- Holzapple, C. W., & Joshi, K. D. (2004). A formal knowledge management ontology: Conduct, activities, resources and influences. Journal of the American Society for Information Science and Technology, 55(7), 593–612 (May).
- ISO/IEC, (2004). Information technology—Security techniques—Information Security Incident Management. Geneva, October. Standard ISO/IEC 18044:2004(E).
- ISO/IEC, (2005). Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model. Geneva, October. Standard ISO/IEC 15408- 1:2005(E).
- ISO/IEC, (2005). Information technology—Security techniques—Information Security Management Systems - Requirements. Geneva, October. Standard ISO/IEC 27001:2005.
- IT Governance Institute (2007). CobiT 4.1 Framework, Control Objectives, Management Guidelines, Maturity Models. Illinois.
- IT Governance Institute (2008). CobiT Control Practices – Guidance to Achieve Control Objectives for Successful IT Governance. 2nd Edition, Illinois.
- IT Governance Institute (2008). Control Objectives for Information and Related Technology - The Val IT Framework. 2nd Edition. Illinois.
- James, R. H. (2003). 1000 anaesthetic incidents: Experience to date. Anaesthesia, 58, 856–863.
- Johnson, C. (2003). Failure in safety-critical systems: A handbook of incident and accident reporting. Glasgow, Scotland: Glasgow University Press.

- Jones, S., Kirchsteiger, C., & Bjerke, W. (1999). The importance of near miss reporting to further improve safety performance. Journal of Loss Prevention in the Process Industries, 12(1), 59–67.
- Kahneman, D. (1973). Attention and effort. Englewood Cliffs, NJ: Prentice-Hall.
- Kahneman, D., & Tversky, A. (2000). Prospect theory: An analysis of decision under risk. In D. Kahneman & A. Tversky (Eds.), Choices, values, and frames. Cambridge, UK: Cambridge University Press.
- Lee, P. I., & Weitzel, T. R. (2005). Air carrier safety and culture: An investigation of Taiwan's adaptation to western incident reporting programs. Journal of Air Transportation, 10(1), 20–37.
- Macfarlane I, Rudd C. (2001). Gestão de Serviços de TI. itSMF. Ltd. Versão 2.1.b.
- National Institute of Standards and Technology. (2001). Engineering principles for information technology security (A baseline for achieving security). Special Publication 800-27. Gaithersburg, MD: US Department of Commerce; 2001 June.
- Nielsen, K. J., Carstensen, O., & Rasmussen, K. (2006). The prevention of occupational injuries in two industrial plants using an incident reporting scheme. Journal of Safety Research, 37(5), 479–486.
- Nyssen, A. S., Aunac, S., Faymonville, M. E., & Lutte, I. (2004). Reporting systems in healthcare from a case-by-case experience to a general framework: An example in anaesthesia. European Journal of Anaesthesiology, 10(21), 757–765.
- O'Dell, C., & Grayson, Jr. C. J. (1998). If only we knew what we know. New York: Free Press.
- Phimister, J. R., Oktem, U., Kleindorfer, P. R., & Kunreuther, H. (2003). Near-miss incident management in the chemical process industry. Risk Analysis, 23(3), 445–459.
- Randazzo, M. R., Keeney, M. M., Kowalski, E. F., Cappelli, D. M., & Moore, A. P. (2004). Insider threat study: Illicit cyber activity in the banking and finance sector. Technical Report. Pittsburgh, PA: U.S. Secret Service and CERT Coordination Center / Software Engineering Institute; 2004 August.
- Repenning, N., & Sterman, J. (2001). Nobody ever gets credit for fixing defects that didn't happen: Creating and sustaining process improvement. California Management Review, 43(4), 64–88.
- Richardson, G. P., & Pugh, A. L. III. (1981). Introduction to system dynamics modeling with DYNAMO. Cambridge MA: Productivity Press.
- Ruivo, J. (2000). ITIL V3. Gestão de serviços em TI.(2010)
- Schneier, B. (2000). Secrets & lies: Digital security in a networked world. Wiley.
- Silva, M., & Martins, J. (2008). *IT Governance, A Gestão da Informática.* FCA..
- Stanhope, N., Crowley-Murphy, M., Vincent, C., O'Connor, A. M., & Taylor-Adams, S. E. (1999). An evaluation of adverse incident reporting. Journal of Evaluation in Clinical Practice, 5(1), 5–12.
- Stanton, J. M., & Stam, K. R. (2006). The visible employee. Medford, MA: Information Today.
- Sterman, J. D. (2000). Business dynamics: Systems thinking and modeling for a complex world. Boston: Irwin McGraw-Hill.

- Stewart, T. A. (1997). Intellectual capital: The new wealth of organizations. New York: Doubleday.
- Sveen, F. O., Rich E., Jager M. (1997). Overcoming organizational challenges to secure knowledge management: Springer Science, 481-492.
- Sveen, F. O., Sarriegi, J.M., Gonzalez, J. (2009). Incident Learning Systems: From Safety to Security: Gjovik University College.
- Sveiby, K. E. (1997). The new organizational wealth: Managing and measuring knowledge-based assets. San Francisco: Berrett Koehler.
- Vargues, Susana (2007). Gestão de Incidentes e Comunicação de Crise. Segurança e Qualidade Alimentar, 40-42.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204.
- Wiik, Johannes, Jose J. Gonzalez, and Klaus-Peter Kossakowski. (2004). Limits to Effectiveness in Computer Security Incident Response Teams. In 23rd International conference of the System Dynamics Society. Oxford.
- Winkler, I. (2005). Spies among us: How to stop the spies, terrorists, hackers, and criminals you don't even know you encounter every day. Indianapolis: Wiley.