



ipai
instituto português de
auditoria interna

Auditoria Interna e Governo das Sociedades

Auditoria Interna e Governo das Sociedades

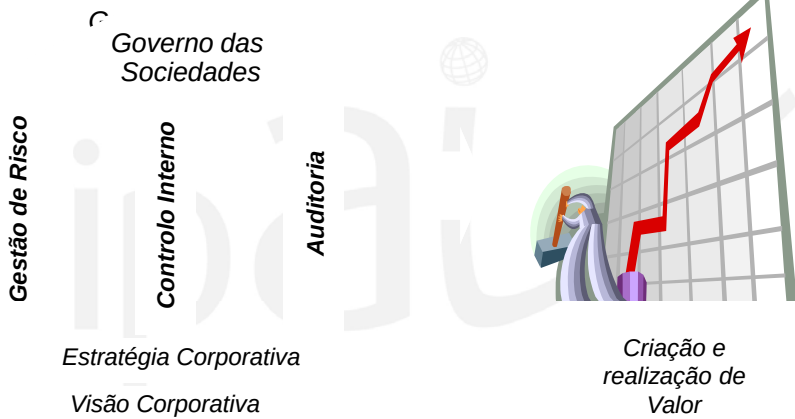
Domingos Sequeira de Almeida, CIA, CCSA

ISCAC, Coimbra, 18 de Setembro de 2010 1



ipai
instituto português de
auditoria interna

Governo das Sociedades



The diagram illustrates the components of Corporate Governance. At the top, 'Governo das Sociedades' is shown. Below it, three vertical pillars are labeled: 'Gestão de Risco' (Risk Management), 'Controlo Interno' (Internal Control), and 'Auditoria' (Internal Audit). These pillars are supported by 'Estratégia Corporativa' (Corporate Strategy) and 'Visão Corporativa' (Corporate Vision). To the right, an illustration shows a person climbing a ladder to reach a target on a grid, with a red arrow indicating the path, labeled 'Criação e realização de Valor' (Creation and realization of Value).

2



Governo das Sociedades

Não existe uma definição padrão de Governo das Sociedades.

A definição mais comum e simples é a seguinte:

‘ Governo das Sociedades é o sistema através do qual as empresas são dirigidas e controladas.’

Cadbury Report - UK 1992

Princípios da OCDE sobre o Governo das Sociedades, 1999

3



Governo das Sociedades

Governo das Sociedades (definição do IIA)

A combinação de processos e estruturas implementados pelo Conselho, para informar, dirigir, gerir e monitorizar as actividades da organização para atingir os seus objectivos.

4



Governo das Sociedades

Códigos do Governo das Sociedades

Alguns exemplos

OECD Principles of Corporate Governance (2004)

*O relato financeiro deve incluir informação relevante sobre (...) os **factores materiais de risco** previstos.*

*O Conselho de Administração deve cumprir com certas funções principais, incluindo: (...) assegurar a existência de **sistemas de controlo** apropriados, em particular, **sistemas de gestão de risco**.*

5



Governo das Sociedades

Códigos do Governo das Sociedades

Alguns exemplos

The Combined Code on Corporate Governance / The Turnbull Guidance (UK, Junho 2008)

*O Conselho de Administração deve manter um sistema prudente de **controlo interno** para salvaguarda do investimento dos accionistas e dos activos da empresa.*

*O Conselho de Administração deve, pelo menos anualmente, dirigir a revisão da efectividade dos **sistemas de controlo interno** e deve reportar aos accionistas que assim o fez. A revisão deve cobrir os **controles** mais relevantes, incluindo os **controles financeiros**, operacionais e de conformidade e os **sistemas de gestão de risco**.*

*As responsabilidades do Comité de Auditoria devem incluir (...) a revisão dos **controles internos financeiros** e dos **sistemas de controlo interno e de gestão de risco**.*

6



Governo das Sociedades

Códigos do Governo das Sociedades

Alguns exemplos

The Sarbanes-Oxley Act (USA-2002)

Sec 404. Management assessment of internal controls

*O relato anual deve conter um **relatório de controlo interno**, que deve:*

- (1) declarar a responsabilidade da gestão no estabelecimento e manutenção de uma **estrutura e procedimentos adequados de controlo interno para reporte financeiro**; e*
- (2) conter uma **avaliação sobre a efectividade da estrutura e procedimentos de controlo interno** para reporte financeiro;*

(...) o auditor externo deve atestar e reportar sobre a avaliação efectuada pela gestão.

7



Governo das Sociedades

Códigos do Governo das Sociedades

Alguns exemplos

Código das Sociedades Comerciais
(revisão de 2006, D-L nº 76-A/2006)

Competência dos Órgãos de Fiscalização

artigos 420º (fiscal único e conselho fiscal), 441º (conselho geral e de supervisão) e 423º-F (Comissão de auditoria):

“Fiscalizar a eficácia do sistema de gestão de riscos, do sistema de controlo interno e do sistema de auditoria interna, se existentes.”

8



Governo das Sociedades

Regulamento da CMVM n.º 1/2010
Governo das Sociedades Cotadas
 (Revogação do Regulamento da CMVM n.º 1/2007)

Anexo I

CÓDIGO DE GOVERNO DAS SOCIEDADES DA CMVM 2010 (RECOMENDAÇÕES)

II. ÓRGÃOS DE ADMINISTRAÇÃO E FISCALIZAÇÃO

II.1. TEMAS GERAIS

II.1.1. ESTRUTURA E COMPETÊNCIAS

II.1.1.2. As sociedades devem criar sistemas internos de controlo e gestão de riscos, em salvaguarda do seu valor e em benefício da transparência do seu governo societário, que permitam **identificar e gerir o risco**. Esses sistemas devem integrar, pelo menos, as seguintes **componentes**:

- i) fixação dos **objectivos estratégicos** da sociedade em matéria de assumpção de riscos;
- ii) **identificação dos principais riscos** ligados à concreta actividade exercida e dos eventos susceptíveis de originar riscos;
- iii) **análise e mensuração do impacto e da probabilidade** de ocorrência de cada um dos riscos potenciais;



9



Governo das Sociedades

- iv) **gestão do risco** com vista ao alinhamento dos riscos efectivamente incorridos com a opção estratégica da sociedade quanto à assunção de riscos;
- v) **mecanismos de controlo** da execução das medidas de gestão de risco adoptadas e da sua eficácia;
- vi) adopção de **mecanismos internos de informação e comunicação** sobre as diversas componentes do sistema e de alertas de riscos;
- vii) **avaliação periódica** do sistema implementado e adopção das modificações que se mostrem necessárias.

II.1.1.3. O **órgão de administração** deve **assegurar a criação e funcionamento dos sistemas de controlo interno e de gestão de riscos**, cabendo ao **órgão de fiscalização** a responsabilidade pela **avaliação do funcionamento destes sistemas** e propor o respectivo ajustamento às necessidades da sociedade.

II.1.1.4. As sociedades devem, no **relatório anual sobre o Governo da Sociedade**:

- i) identificar os principais riscos económicos, financeiros e jurídicos a que a sociedade se expõe no exercício da actividade;
- ii) descrever a actuação e eficácia do sistema de gestão de riscos.



10



Governo das Sociedades

European corporate governance institute: www.ecgi.org/codes ¹



europaean corporate governance institute

[HOME](#)
[CONTACT US](#)
[SEARCH](#)
[MEMBERS](#)
[SITE MAP](#)
[DISCLAIMER](#)

[ABOUT SITE](#)

Index of codes

choose a countrv....

¹ Este site contém um repositório dos códigos e documentos de Governo das Sociedades de dezenas de países e organizações

11



Governo das Sociedades

European corporate governance institute: www.ecgi.org/codes

EXEMPLO

 **Portugal**

- [CMVM Corporate Governance Code 2010 \(Recommendations\)](#) 8 January 2010
- [CMVM Corporate Governance Code](#) September 2007
- [Proposal on the Corporate Governance Code](#) 3 April 2007
- [White Book on Corporate Governance in Portugal](#) February 2006
- [Recommendations on Corporate Governance](#) November 2003
- [CMVM Regulation N° 11/2003: Corporate Governance](#) 2003
- [CMVM Regulation No 07/2001: Corporate Governance](#) December 2001
- [Recommendations on Corporate Governance](#) November 1999

12

Controlo Interno

Definição de Controlo Interno

Definição do “COSO - Internal Control Integrated Framework” (1992):

O Controlo Interno é um **processo**, desenvolvido pela Administração, Gestão e outros colaboradores da Organização, desenhado para permitir uma segurança razoável na realização dos seguintes objectivos (categorias):

Eficácia e eficiência das operações

Fiabilidade do reporte financeiro

Conformidade com as leis e regulamentos aplicáveis

13

Gestão de Risco

DEFINIÇÃO

A Gestão de Risco empresarial é um processo, desenvolvido pela Administração, a Gestão e outros colaboradores de uma entidade, aplicado no estabelecimento da estratégia em toda a empresa, desenhado para identificar eventos potenciais que possam afectar a entidade, e gerir o risco dentro da apetência de risco da entidade, para garantir uma segurança razoável na realização dos objectivos.

Enterprise Risk Management Framework – COSO

(www.coso.org)

14



Auditoria Interna

Definição de Auditoria Interna

*A auditoria interna é uma actividade independente, de garantia e de consultoria, destinada a acrescentar valor e a melhorar as operações de uma organização. Ajuda a organização a alcançar os seus objectivos, através de uma abordagem sistemática e disciplinada, na **avaliação e melhoria da eficácia dos processos de gestão de risco, de controlo e de governação**.*

(definição do IIA – The Institute of Internal Auditors traduzida pelo IPAI - Instituto Português de Auditoria Interna)

15



Auditoria Interna

A importância da Auditoria Interna na Gestão e Governo das Sociedades

Auditoria Interna: um dos pilares do Governo das Sociedades

A Auditoria Interna deve contribuir para:

- Desenvolvimento de um ambiente de Controlo Interno
- Transparência das relações entre a Gestão e a Administração
- Combate à Fraude
- Melhoria do reporte financeiro e de gestão
- Reporte de informação para a Administração e Comité de Auditoria sobre a gestão de risco e controlo interno

16



Auditoria Interna

A importância da Auditoria Interna na Gestão e Governo das Sociedades

Ética nos negócios e ambiente de Controlo Interno

A Auditoria Interna deve contribuir para a melhoria da Ética nos negócios e do ambiente de Controlo Interno, através de:

- Identificação e reporte de situações efectivas e potenciais de fraude*
- Prevenção e inibição de comportamentos fraudulentos*
- Recomendação de boas práticas de gestão e de controlo*
- Promoção e participação em projectos e iniciativas de desenvolvimento de políticas e procedimentos de Controlo Interno*

17



Auditoria Interna

A importância da Auditoria Interna na Gestão e Governo das Sociedades

Controlo dos Riscos de negócio

A Auditoria Interna deve avaliar a efectividade dos processos de gestão de risco, através de:

- Actividade (planeamento, execução e reporte das auditorias) baseada na análise dos riscos dos processos e sistemas de negócio*
- Contribuição para o desenvolvimento dos processos de gestão de riscos, nomeadamente: riscos operacionais, financeiros e de sistemas de informação*

18



Auditoria Interna

A importância da Auditoria Interna na Gestão e Governo das Sociedades

Performance dos negócios

A Auditoria Interna deve contribuir para a melhoria da performance dos negócios:

Recomendações para a eficácia e eficiência dos processos e sistemas de negócio

Prevenção da fraude

Reporte sobre riscos potenciais de perda de valor para a organização, p.e.:

- Riscos de crédito e de cobrança
- Riscos de roubo ou de ineficiente utilização dos recursos

19



Auditoria Interna

A importância da Auditoria Interna na Gestão e Governo das Sociedades

Auditoria dos Sistemas e Tecnologias de Informação

Importância acrescida dos sistemas e tecnologias de informação na gestão dos negócios;

Dependência cada vez maior da informação para a tomada de decisão;

Aumento do nr. de pessoas e do "apetite" ao acesso indevido a informação confidencial das Empresas;

Consequências potencialmente graves na continuidade dos negócios.

T

Necessidade acrescida do controlo dos riscos de sistemas e tecnologias de informação através do desenvolvimento de auditorias especializadas.

20



Auditoria Interna

A importância da Auditoria Interna na Gestão e Governo das Sociedades
Auditorias de Segurança, Higiene e Saúde e Ambiente

Numa perspectiva de:

- **Sustentabilidade** dos negócios;
- **Responsabilidade Social**;
- **Gestão mais abrangente** dos riscos das organizações.

Auditoria Interna deve contribuir para a melhoria do controlo dos riscos de:

- Segurança física das pessoas e instalações;
- Segurança alimentar;
- Higiene e Saúde no trabalho;
- Ambiente.

Através de:

Actividade geral de auditoria e consultoria e/ou
Auditorias Internas especializadas

21



Auditoria Interna

A importância da Auditoria Interna na Gestão e Governo das Sociedades
Auditoria Interna: conforto e garantia nos processos de gestão

- ♦ Papel relevante na **criação e consolidação da confiança** dentro da organização;
- ♦ Factor de **conforto e garantia** no controlo dos riscos;
- ♦ Promove o **alinhamento** de todos os níveis da Organização;
- ♦ Facilitador da **descentralização** da gestão, delegação e autonomia das funções;
- ♦ Mecanismo de **optimização** e de **evolução qualitativa** da gestão: identificar, questionar e melhorar ineficiências;
- ♦ Potenciador de **inovação**: permite assumir mais risco e aproveitar oportunidades.

22

2110 – Governação

A actividade de auditoria interna tem que **avaliar e efectuar recomendações** apropriadas para a **melhoria do processo de governação**, no cumprimento dos seguintes objectivos:

- Promover a **ética e valores** apropriados no seio da organização;
- Assegurar a **gestão do desempenho organizacional** e sua responsabilização de forma eficaz;
- Transmitir de forma eficaz a **informação sobre risco e controlo**, às áreas apropriadas da organização;
- Coordenar eficazmente as actividades de **comunicação e informação ao Conselho, aos auditores externos e internos e aos gestores.**

23

2110 – Governação (cont.)

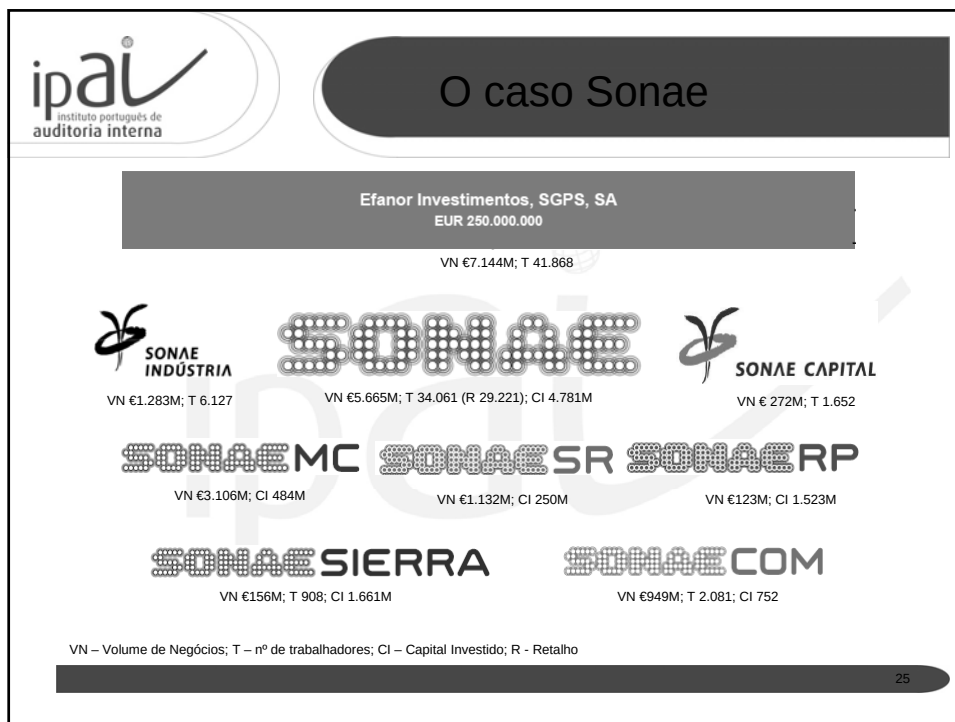
2110.A1 – A actividade de auditoria interna tem que **avaliar** o desenho, implementação e eficácia dos **objectivos, programas e actividades** da organização relacionados com a **ética**.

2110.A2 – A actividade de auditoria interna tem que **avaliar** se a **governança das tecnologias de informação** da organização mantém e apoia as estratégias e os objectivos da organização.

2110.C1 – Os objectivos dos compromissos de consultoria deverão ser consistentes com os valores e as metas globais da organização.

Associados

24



ipai
instituto português de
auditoria interna

O caso Sonae

SONAE
Turnover 5.7 billion euros (2009); EBITDA 667 million euros (2009); Invest Capital 4.8 billion euro (2009)

100%	100%	100%	50%	53%	100%
SONAE MC Food Retail	SONAE SR Specialised Retail	SONAE RP Retail Properties	SONAE SIERRA Shopping Centres	SONAE COM Telco	Investment Management
Hipers and Supers	Non-Food Retail formats: Sports, Textiles and Electronics	Retail Real Estate assets	Shopping centre developer, owner and manager	Integrated Telecom provider	Business with M&A activity: Insurance, Travel And DIY
55% Sales 30% EBITDA 10% Inv. Capital	20% Sales 7% EBITDA 5% Inv. Capital	2% Sales 17% EBITDA 32% Inv. Capital	3% Sales 14% EBITDA 35% Inv. Capital	17% Sales 26% EBITDA 16% Inv. Capital	3% Sales 4% EBITDA 3% Inv. Capital
CORE BUSINESS		RELATED BUSINESS	CORE PARTNERSHIP		ACTIVE INVESTMENT

26



O caso Sonae

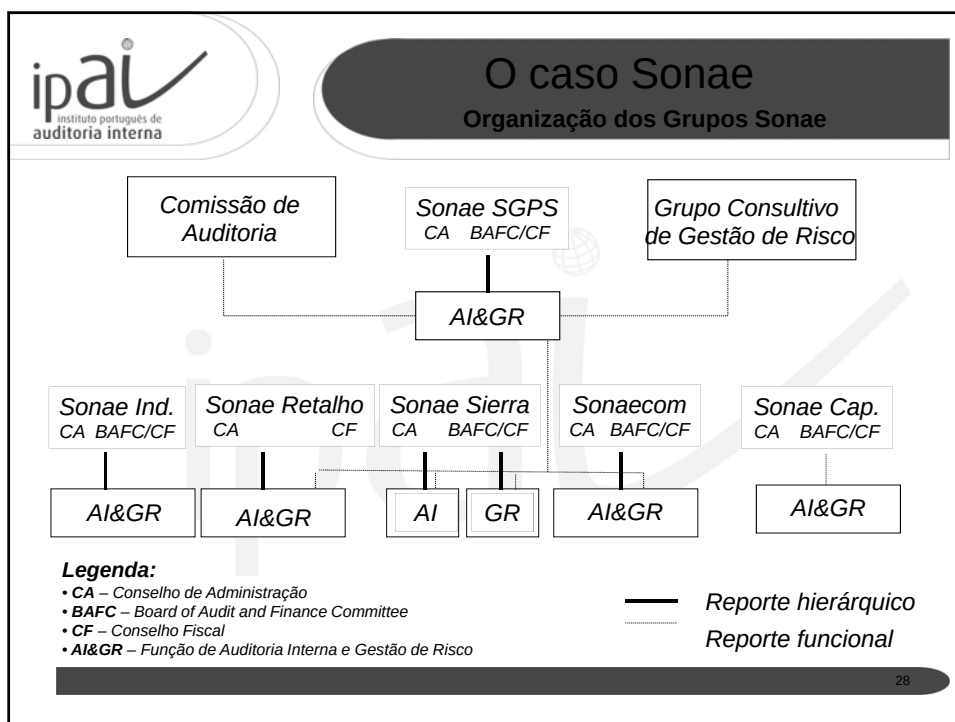
Gestão de Risco e Auditoria Interna

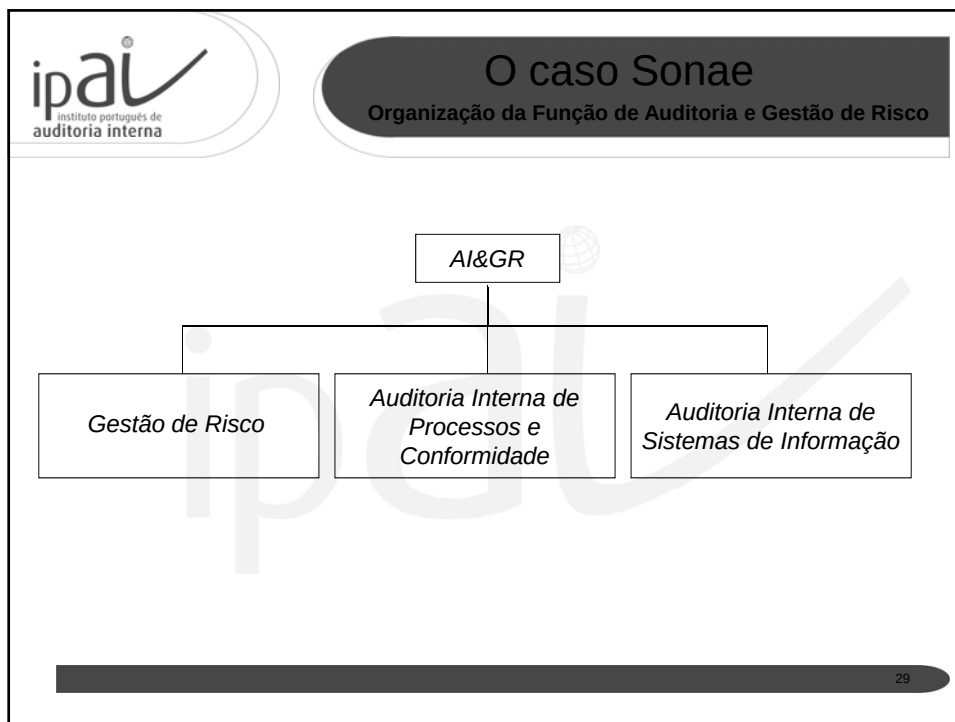
Missão:
 Ajudar a organização a atingir os seus objectivos através de uma abordagem sistemática e disciplinada para avaliar e promover a efectividade dos processos de gestão de risco, controlo e governo da sociedade.

Responsabilidades:

- Identificar e avaliar a efectividade da gestão de risco e do controlo:
 - Riscos dos processos e sistemas de informação de negócio;
 - Riscos de conformidade: legais, contratuais, políticas e procedimentos de controlo interno.
- Promover e suportar a cultura, metodologias e processos de gestão de risco.

27





ipai
instituto português de
auditoria interna

O caso Sonae

Organização da Função de Auditoria e Gestão de Risco

Órgãos de Partilha e Conhecimento
Comissão de Auditoria e Grupo Consultivo de Gestão de Risco (GCGR):

Funções:
Órgãos, ao nível do Grupo, que assistem os Conselhos de Administração e coordenam as actividades de Auditoria e Gestão de Risco (AGR):

- Definem e propõem as políticas de AGR;
- Revêem e coordenam as actividades de Gestão de Risco e de Auditoria;
- Revêem os processos e sistemas de gestão de risco e controlo interno;
- Fora de partilha de conhecimento e experiência.

Membros:

- Membros dos Conselhos de Administração com o pelouro e Directores de AGR da Holding e Sub-holdings;

30



O caso Sonae

Âmbito da Gestão de Risco

- Riscos do ambiente de negócio (mercado, concorrência, regulação, ...)
- Riscos dos processos de negócio:
 - Riscos operacionais (eficiência, capacidade, recursos humanos, satisfação dos clientes, ...)
 - Riscos de "autorização" (liderança, limites de autorização, preparação para a mudança, ...)
 - Riscos dos sistemas e tecnologias de informação
 - Riscos de integridade (reputação, fraude, actos ilegais, uso não autorizado,...)
 - Riscos financeiros
- Riscos da informação para a tomada de decisão
- Riscos físicos e seguráveis:
 - Segurança das pessoas
 - Danos patrimoniais
 - Interrupção do negócio

31



O caso Sonae

Âmbito da Auditoria Interna

- Riscos dos processos de negócio
- Riscos de conformidade:
 - Legislação e contractos
 - Políticas e procedimentos de controlo interno
 - Políticas e procedimentos de Gestão Ambiental, Saúde e Segurança (SHE)
- Riscos financeiros:
 - Caixa e bancos
 - Cobranças e pagamentos
 - Créditos
- Riscos dos sistemas e tecnologias de informação:
 - Disponibilidade
 - Integridade
 - Segurança física
 - Desempenho e qualidade

32

O caso Sonae

Equipas de Auditoria Interna e Gestão de Risco

	DIR	APC	ASI	GR	Total
Sonae	1	21*	3**	2	27
Sonae Sierra	1	3	**	***	4
Sonaeacom	1	4	2	2	9
Total Grupo Sonae	3	28	5	4	40
Sonae Indústria	1	3	**	2	6
Sonae Capital	1	1	**		2

* Inclui Auditoria de Segurança Alimentar (5) e Monitorização (3)

** Inclui um auditor partilhado com Sonae Sierra, Sonae Indústria and Sonae Capital

*** Grupo de Trabalho de Gestão de Risco

Legenda:

DIR - Director

APC - Auditoria de Processos e Conformidade;

ASI - Auditoria de Sistemas de Informação;

GR - Gestão de Risco

33

O caso Sonae

Equipas de Auditoria Interna e Gestão de Risco

Certificação Profissional

Nº de certificações nas equipas de Auditoria Interna e Gestão de Risco:

										
Certified	11	9	4	2	1	1	1	3	1	1

CIA - Certified Internal Auditor (IIA - The Institute of Internal Auditors);

CCSA - Certification in Control Self-Assessment (IIA - The Institute of Internal Auditors);

CISA - Certified Information Systems Auditor (ISACA - Information System Audit and Control Association);

ISMS - Certification in Information Security Management System BS ISO/IEC 27001:2005 (British Standards Institution);

CISSP - Certified Information System Security Professional (International Information Systems Security Certification Consortium);

BS 25999 - Business Continuity Management (British Standards Institution);

ABCP - Associate Business Continuity Professional (DRII - Disaster Recovery Institute International);

CISM - Certified Information Security Management (ISACA - Information System Audit and Control Association);

PMI - Project Management;

BCI - Certified by Business Continuity Institute (BCI - Business Continuity Institute)

34



Informação na internet

AUDITORIA INTERNA:

- The Institute of Internal Auditors (IIA): www.theiia.org
- European Confederation of Institutes of Internal Auditing – ECIIA: www.eciia.org
- IPAI - Instituto Português de Auditores Internos: www.ipai.pt
- Information Systems Audit and Control Association and Foundation: www.isaca.org

GESTÃO DE RISCO:

- FERMA - Federation of European Risk Management Associations : www.ferma-asso.org
- IFRIMA - The International Federation of Risk and Insurance Management : www.rims.org/ifrima/
- AIRMIC - The Association of Insurance and Risk Managers: www.airmic.com
- APOGERIS – Associação Portuguesa de Gestão de Riscos e Seguros: www.apogeris.pt

CORPORATE GOVERNANCE:

- Corporate Governance : www.corpgov.net
- European Corporate Governance Institute: www.ecgi.org
- The International Corporate Governance Network: www.icgn.org
- Global Corporate Governance Forum : www.gcgf.org
- Instituto Português de Corporate Governance: www.cgov.pt

GERAIS:

- COSO : www.coso.org