Inquérito Aberto à Segurança da Informação nas Instituições em Portugal

- 1ª Edição –

Sumário

Promovido por:

Com a colaboração de:

ISCTE IUL
Instituto Universitário de Lisboa

Com o apoio de:

EMPRESAS FAMILIARES
Associação das Empresas Familiares
Portuguese Family Businesses

ADSP
Associação dos Directores de Segurança de Portugal

Índice

Introdução

É com bastante satisfação que a AP2SI apresenta o resultado do seu primeiro **Inquérito Aberto à Segurança da Informação nas Instituições em Portugal**.

A nossa motivação para a realização deste inquérito partiu da necessidade de existirem números concretos relativos à realidade portuguesa. Por outro lado procurámos oscultar não apenas os responsáveis de IT ou segurança nas organizações, mas também outros colaboradores – em cargos de direção ou não – de modo a construir uma visão mais completa da percepção existente atualmente. À medida que as ameaças à segurança da informação se tornam mais comuns e presentes no nosso dia-a-dia entendemos que é importante perceber de que modo as organizações estão a responder aos desafios tecnológicos mas, talvez mais importante, aos desafios culturais e organizacionais.

O inquérito cobriu diversos aspetos que entendemos como fundamentais para a criação de uma cultura de segurança de informação eficaz nas instituições, nomeadamente:

- O compromisso da gestão de topo;
- A formação de competências;
- A existência de uma unidade organizacional dedicada;
- O papel da auditoria e controlo;
- A gestão de incidentes de segurança.

Adicionalmente sentimos também a necessidade de aprofundar alguns dos temas com o ponto de vista da camada diretiva e da gestão, mais especificamente sobre:

- A gestão do orçamento para Segurança da Informação;
- A gestão dos recursos humanos com funções na Segurança de Informação;
- A existência de incidentes e eventuais perdas relacionadas;
- As preocupações de segurança dos orgãos de topo;
- A percepção da exposição da instituição às ameaças.

Pretendemos assim ter uma ideia generalizada de que modo as organizações entendem o tema da Segurança da Informação e de que modo o colocam em prática, sendo nosso objetivo que este trabalho possa ajudar a entender a realidade em Portugal e sirva como referência para o aumento da consciencialização para o tema da Segurança da Informação nas instituições a operar no nosso país.

Os resultados do Inquérito estão divididos em dois documentos:

- Este **Sumário** onde são apresentadas as principais conclusões;
- A **Análise de Resultados**, levada a cabo pelo Departamento de Matemática, da Escola de Tecnologias e Arquitectura do ISCTE-IUL.

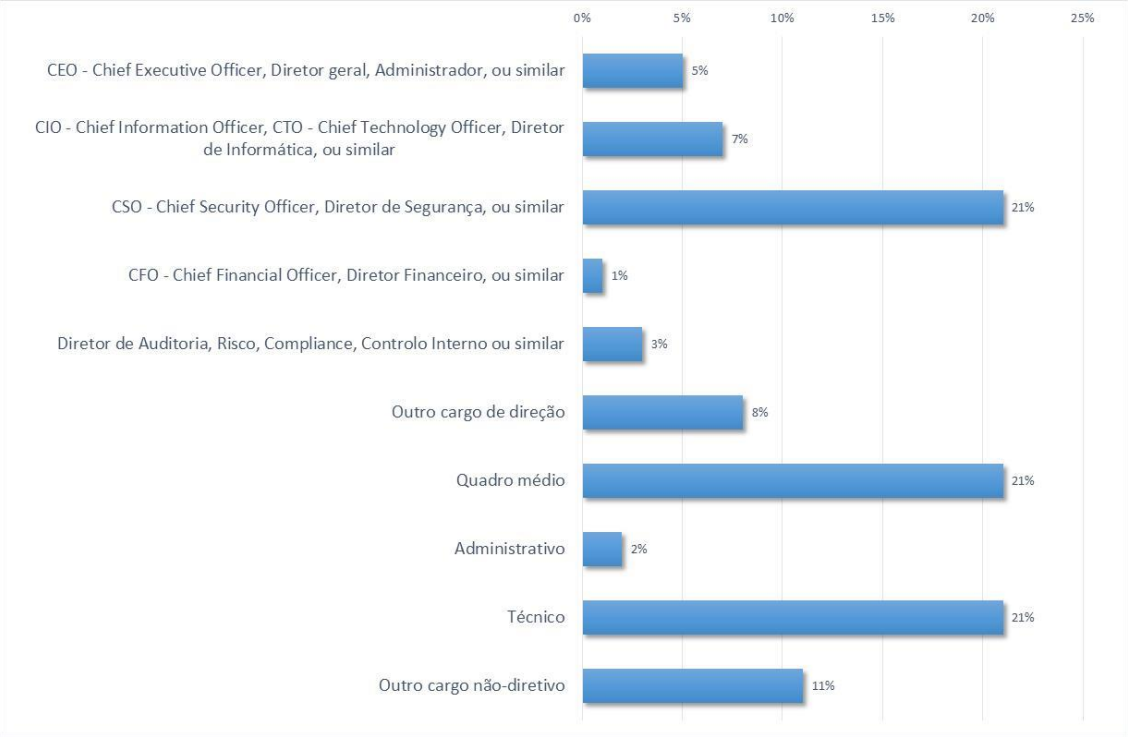
Ambos os documentos estão disponíveis gratuitamente no sítio da AP2SI em https://ap2si.org/inquerito. Para mais informações contacte geral@ap2si.org.

Sumário dos Resultados Obtidos

Quem respondeu ao inquérito?

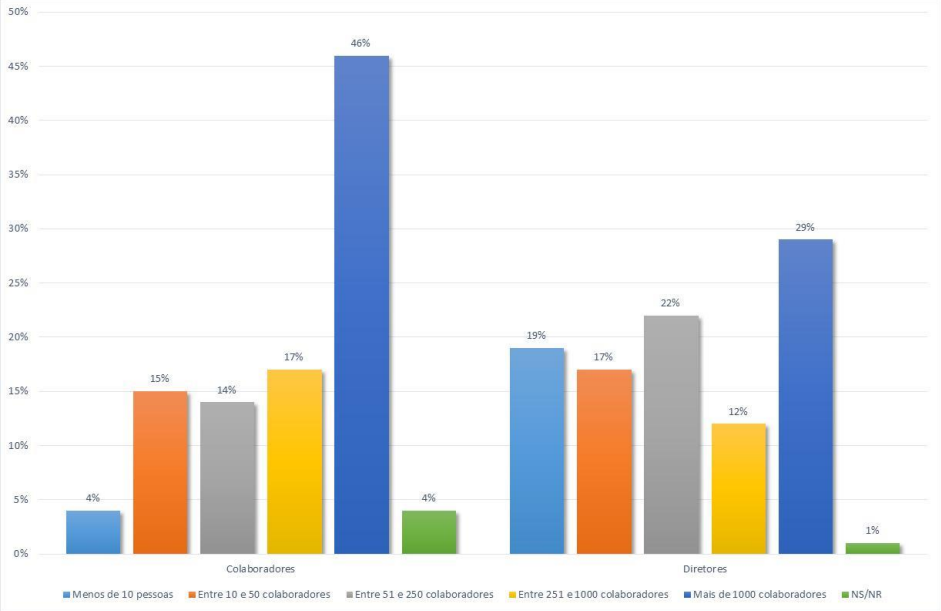
O **Inquérito Aberto à Segurança da Informação nas Instituições em Portugal** foi aplicado a 169 indivíduos de diferentes setores e desempenhando diferentes funções nas suas instituições. Destes, 150 (88,8%) desenvolvem a sua atividade profissional numa instituição em Portugal. Como tal, as restantes questões foram aplicadas apenas a estes últimos.

Um dos objetivos desta iniciativa foi conseguir respostas de vários níveis das instituições e entendemos que foi atingido, pela variedade de cargos indicados, como se pode ver no gráfico seguinte.

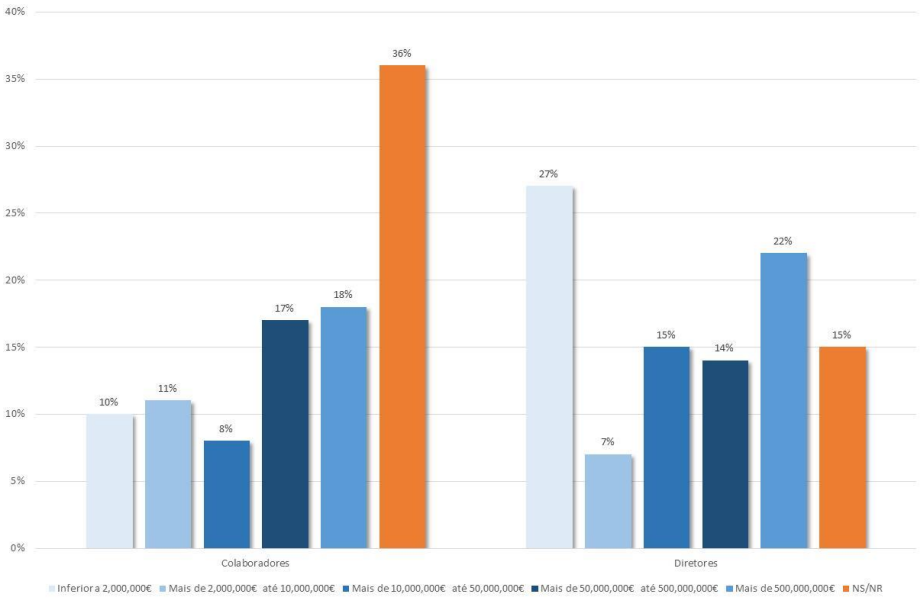


Identificação dos cargos exercidos

A percepção da dimensão da instituição foi um fator de preocupação a par do volume de negócios. Os seguintes gráficos apresentam a distribuição das respostas prestadas tendo em conta estas duas dimensões.



Número de respostas por dimensão da instituição

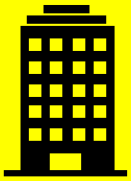


Número de respostas por volume de negócios

Também o setor de atuação é relevante, estando representados vários setores da economia com destaque para **Serviços e produtos de telecomunicações e tecnologias de informação** (27,8%), **Administração central e orgãos do estado** (14,3%), **Investigação e segurança, prestação de serviços de segurança privada** (12,8%) e **Instituições bancárias, locação financeira, seguros e afins** (10,5%).

A Política de Segurança da Informação e o envolvimento da Gestão de Topo

O compromisso da gestão de topo com a segurança da informação pode ser evidenciado, primariamente, pela existência de uma Política de Segurança da Informação que espelhe qual a visão que a instituição pretende aplicar com respeito à segurança da informação de que é proprietária ou a que venha a ter acesso.



55,2% dos colaboradores e 75,5% dos diretores indicam que existe uma política de segurança da informação na instituição

Em relação à existência de uma uma política de segurança da informação na instituição 55,2% dos colaboradores indicaram a sua existência, assim como 75,5% dos diretores. Quando esta existe, 73,3% dos colaboradores reportaram que foi emitida pela gestão de topo, assim como 83,8% dos diretores.

A existência de uma política é apenas um pilar da cultura de segurança da informação das instituições. Não basta que exista apenas um documento, é necessário também que exista um compromisso visível. Quando questionados sobre se **a segurança da informação é uma preocupação da gestão de topo** 71,6% dos colaboradores e 81,1% dos diretores respondem afirmativamente.

28,4% dos colaboradores e 24,5% dos diretores trabalha em instituições certificadas numa norma de gestão de segurança da informação

No entanto **apenas** 28,4% dos colaboradores e 24,5% dos diretores trabalham em instituições certificadas numa norma de gestão de segurança da informação.

O método mais comum de manifestação de apoio à política de segurança pela gestão de topo é **a liderança pelo exemplo** de acordo com 60% dos colaboradores e 56,8% dos diretores. No entanto existe uma **fraca participação** em comités de segurança ou similares sendo esta opção apontada apenas por 30% dos colaboradores e 35% dos diretores.

No que diz respeito à periodicidade de revisão da política apenas 50% dos colaboradores indica que sabe quando esta é revista: 17,9% indica **sempre que existem alterações na instituição**, valor igual aos que indicam que esta **ocorre uma vez por ano** e 7,1% avança que a política é **revista de dois em dois anos**. Já os diretores são mais assertivos com 45,9% a responder que a revisão ocorre **sempre que existam alterações** e 40,5% indicam **pelo menos uma vez por ano**.

É de realçar também as situações em que a política de segurança nunca foi revista sendo tal identificado por 7,1% dos colaboradores e 8,1% dos diretores.

Apesar da maioria das respostas indicar a existência de uma política de segurança nas instituições **nem sempre esta é do conhecimento de todos os colaboradores**. Apenas 56,7% dos colaboradores indicam que conhecem a política, valor que contrasta com os 70,3% dos diretores que responderam positivamente.

A Sensibilização e a Formação em Segurança da Informação

Os temas da sensibilização e da formação em Segurança da Informação são cruciais para a implementação e manutenção de uma cultura de segurança nas instituições. Em questões de segurança o conhecimento é a chave para a tomada de decisões correctas e quanto mais disseminado estiver maior a resiliência das instituições.

De acordo com as respostas recebidas esta é claramente uma das áreas deficitárias nas instituições: Apenas 30% dos colaboradores e 31,5% dos diretores trabalha em instituições onde **é ministrada formação em segurança da informação**. Nestes casos a formação é ministrada **maioritariamente** de **forma regular a todos os colaboradores** destacando-se os temas das boas práticas na utilização de sistemas de informação, as boas práticas no manuseamento da informação, a construção de passwords e como agir em caso de incidentes.

A Organização de Segurança da Informação

A segurança não é um produto, mas antes um processo. De forma a assegurar a capacidade de gerir adequadamente o tema dentro das instituições é necessário que existam recursos alocados ao mesmo.

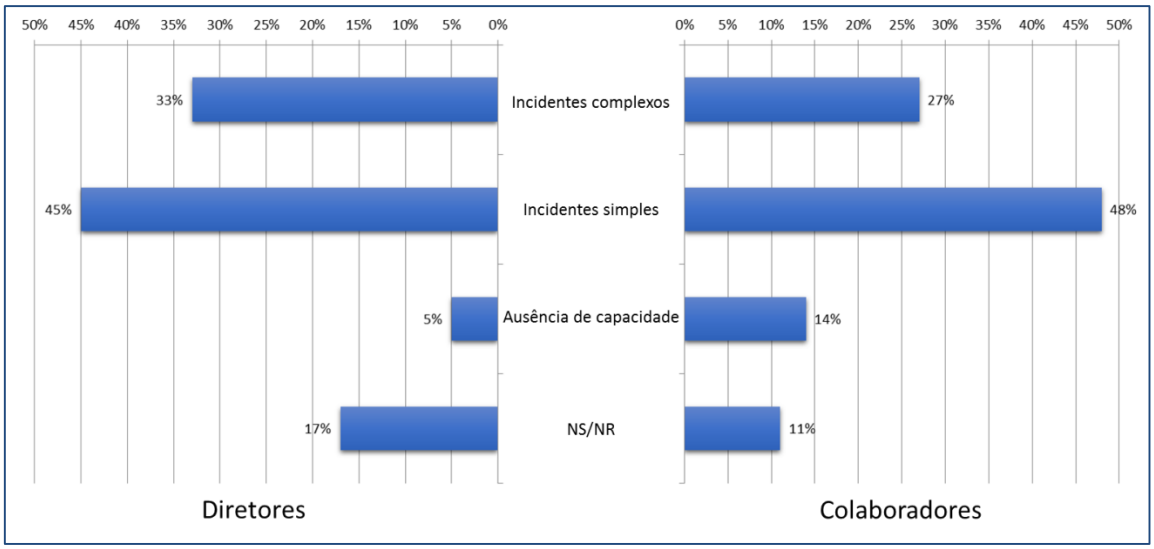
No caso das instituições portuguesas as respostas não são encorajadoras sendo que menos de metade das respostas indica a existência de uma organização de segurança: 45,8% dos colaboradores e 47,8% dos diretores responderam **afirmativamente** à questão. A dificuldade de contratar profissionais nesta área poderá estar na origem desta falha uma vez que 31% dos diretores indicam que é **muito difícil** contratar um profissional especializado em segurança da informação, ao passo que 24,1% indicam que é **razoavelmente difícil**. Apenas 6,9% indicam que é **razoavelmente fácil** a contratação de um profissional nesta área. Também as questões orçamentais poderão concorrer para a dificuldade em manter uma organização de segurança da informação. Quando questionados sobre a existência de um orçamento específico para segurança da informação, as respostas dos diretores dividiram-se equitativamente com 40,9% a indicar **positivamente** a sua existência e 40,9% com indicação **negativa**. 18,2% não sabe ou não responde. No entanto para os que responderam positivamente 35,5% dos diretores indicam que o orçamento alocado à segurança da informação **constitui menos de 1% do orçamento da instituição** com 41,9% indicando que não sabe ou não responde.

Mais dificuldades se avizinham para 2016 com apenas 11,9% dos diretores a prever um aumento do orçamento de segurança.

Incidentes de Segurança da Informação

Cada vez mais as instituições necessitam de desenvolver a capacidade de detetar atempadamente e responder de forma eficaz a incidentes de segurança de forma a proteger a sua informação e a dos seus clientes.

A maioria dos inquiridos – colaboradores ou diretores – entende que a instituição tem **capacidade para detetar e responder em tempo útil** a incidentes, embora sejam mais otimistas quanto mais simples for o incidente.



No entanto é também possível notar a diferença entre colaboradores e diretores relativamente ao conhecimento dos procedimentos em vigor no caso de se tornarem vítimas de um ataque: 71,4% dos diretores indicaram conhecer os procedimentos em vigor na instituição para atuação no caso de ser vítima de um ataque contra 37,5% dos colaboradores.

Estes valores tomam maior significado quando 23,8% dos diretores e 26,8% dos colaboradores indicam que já foram pessoamente visados por ataques.

Quando questionados sobre o tipo de incidentes detetados mais frequentemente, os **Ataques a sítios de Internet da instituição** ocupam o primeiro lugar nas respostas, seguidos de ***Hacking* ou intrusão na rede** e ***Phishing* ou *Spearphising***.

26% dos diretores afirmam que a sua **instituição já foi vítima de ataques bem-sucedidos** e 41% indicam que não sabem ou não respondem.

As Preocupações da Gestão de Topo

Qualquer instituição que não mantenha os olhos no futuro corre o risco de se deixar ultrapassar. Tal também é verdade nos domínios da segurança da informação – não estar consciente dos riscos possíveis implica que estes não serão estudados, entendidos ou controlados aumentando a probabilidade da instituição se tornar uma vítima.

Tentámos, através deste inquérito perceber o que deixa a camada de direção das instituições portuguesas acordada à noite. Foram obtidas respostas de 42 diretores relativamente a um conjunto de temas, sendo as respostas indicadas na tabela seguinte, ordenadas pelo tema de maior preocupação.

Pelas respostas disponibilizadas é possível perceber que **as questões de segurança são indissociáveis do negócio** das instituições.

Tema	Menor preocupação				Maior preocupação
Incapacidade de assegurar o serviço prestado a clientes	7	2	6	8	**18**
Indisponibilidade dos sistemas imprescindíveis ao negócio	3	4	7	11	**16**
Disseminação pública não autorizada de informação da instituição	2	3	11	10	**15**
Roubo de informação de negócio / propriedade intelectual	3	5	9	9	**15**
Falta de capacidade de deteção de ataques	2	7	9	9	**14**
Proteção de dados pessoais e dados pessoais sensíveis	2	5	11	9	**14**
Ataques de hackers ou organizações criminosas	5	6	7	10	**13**
Desconhecimento das ameaças	4	5	9	10	**13**
Ataques de negação de serviço que ataquem canais de negócio e comunicação com o cliente	6	5	8	10	**12**
Cumprimento com legislação e outras obrigações regulamentares	6	5	6	15	**9**
Falta de capacidade orçamental	4	9	12	8	**8**

Tema	Menor preocupação				Maior preocupação
Falta de pessoal especializado	5	9	10	10	**7**
Software malicioso (vírus, worms, cavalos de Tróia, etc.)	3	5	10	16	**7**
Cloud computing	11	4	12	8	**6**
Shadow IT (sistemas utilizados pela instituição mas desconhecidos pela área de gestão de SI)	5	12	10	8	**6**
Segurança na cadeia de fornecimento (serviços e produtos)	8	3	16	9	**5**

Foram também encontradas fortes correlacões nas preocupações com a gestão de recursos, nomeadamente:

- restrições orçamentais,
- dificuldade em contratar pessoal especializado e,
- *shadow IT*.

Também correlacionadas entre si estão as preocupações com a segurança na cadeia de fornecimento e o *cloud computing*.

Conclusões

Embora esta seja a primeira edição desta iniciativa os resultados já sugerem que nas instituições tanto colaboradores como gestores estão conscientes de alguns riscos sendo também visível que os cargos associados à gestão e direção estão conhecedores de alguns dos temas tratados no inquérito.

No panorama atual as instituições devem conseguir olhar além do modo como desenvolvem o seu negócio e garantir que desenvolvem também as capacidades necessárias para analisar e percepcionar as novas ameaças a que estão sujeitas, das quais as ameaças à sua informação são apenas uma parte. Quem conseguir dar este passo estará a trabalhar não só para melhorar a sua segurança mas também para dinamizar o modo como se inserem no tecido económico, social e tecnológico, graças a uma maior visibilidade dos riscos a que estão sujeitas.

No entanto os resultados sugerem que, para os orgãos de gestão, estes riscos ainda não justificam a adoção de medidas específicas como a contratação de pessoal especializado ou a criação de unidades orgânicas nas instituições que estejam inteiramente dedicadas ao tema, sendo que é patente a falta de recursos dedicados e, em alguns casos as diferenças de perceção entre colaboradores e diretores.

A AP2SI entende que a mudança cultural é algo que demorará tempo mas reforça que este tempo vai ser cada vez mais curto. Os modos como trabalhamos, transmitimos e armazenamos a informação estão constantemente a evoluir e as instituições que não se conseguirem adaptar estarão a colocar em causa o seu futuro.

Numa nota final queremos deixar os nossos agradecimentos a todos os que participaram e também aos que se juntaram a esta iniciativa - a contribuição valiosa do **Departamento de Matemática, da Escola de Tecnologias e Arquitectura do ISCTE-IUL** para a análise aprofundada dos resultados e o trabalho de divulgação realizado pela **AEF – Empresas Familiares** e pela **ADSP – Associação dos Diretores de Segurança de Portugal**.

Sobre a AP2SI:

A AP2SI – Associação Portuguesa para a Promoção da Segurança da Informação – AP2SI foi fundada em Janeiro de 2012, é uma associação sem fins lucrativos e de natureza privada e tem como objetivo contribuir para o desenvolvimento da Segurança da Informação em Portugal, de forma activa, através da sensibilização para o valor e necessidade de protecção da Informação, e do desenvolvimento e promoção de orientações que visem reforçar o conhecimento e a qualificação dos indivíduos e organizações.

Visite-nos em **https://ap2si.org** ou contacte-nos em **geral@ap2si.org**.

I Inquérito à Segurança da Informação nas Instituições em Portugal

1ªedição – Abril de 2016