WORKSHOP 4

SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

43º COLÓQUIO DA QUALIDADE

Porto Business School, 24 outubro 2018

Fazer acontecer. A Qualidade em Ação

APQ

SGS

SESSÃO DE ABERTURA

WHEN YOU NEED TO BE SURE

SGS

A GESTÃO DO RISCO DA INFORMAÇÃO

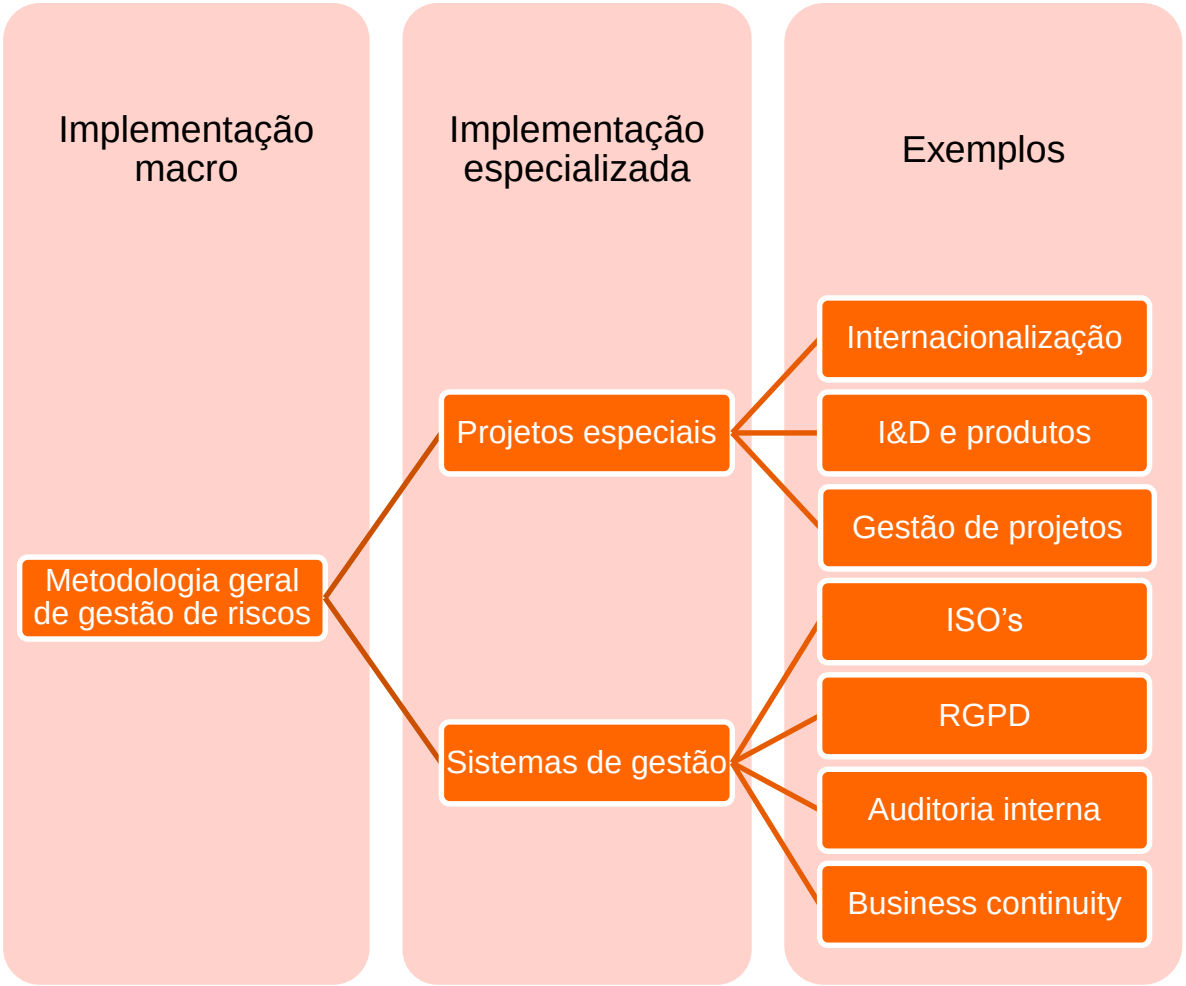
SÉRGIO RESENDE - SGS

WHEN YOU NEED TO BE SURE

SGS

ENQUADRAMENTO DA METODOLOGIA GESTÃO DE RISCOS

ALCANCE DA GESTÃO DE RISCOS



ESTUDO DE CASOS
NO ÂMBITO DA SEGURANÇA DE INFORMAÇÃO

Ocorrência: Ataque Hacker ao sistema de dados da marca Japonesa, provocando acesso indevido a dados pessoais, incluindo user-names e passwords de cliente.

Que ilações retirar?

- Quais as causas da ocorrência?
- Quais as consequências para os clientes?
- Qual o impacto no negócio (inclusive ao nível da performance)?
- O risco nunca será zero;
- Cada caso dever ter o seu sistema, este deve ser efetivo e não apenas uma ideia bonita.

BARREIRAS E OPORTUNIDADES DA IMPLEMENTAÇÃO

A ISO 27001

NUNO OLIVEIRA – INTEGRITY

WHEN YOU NEED TO BE SURE

SGS

/// Colóquio da Qualidade

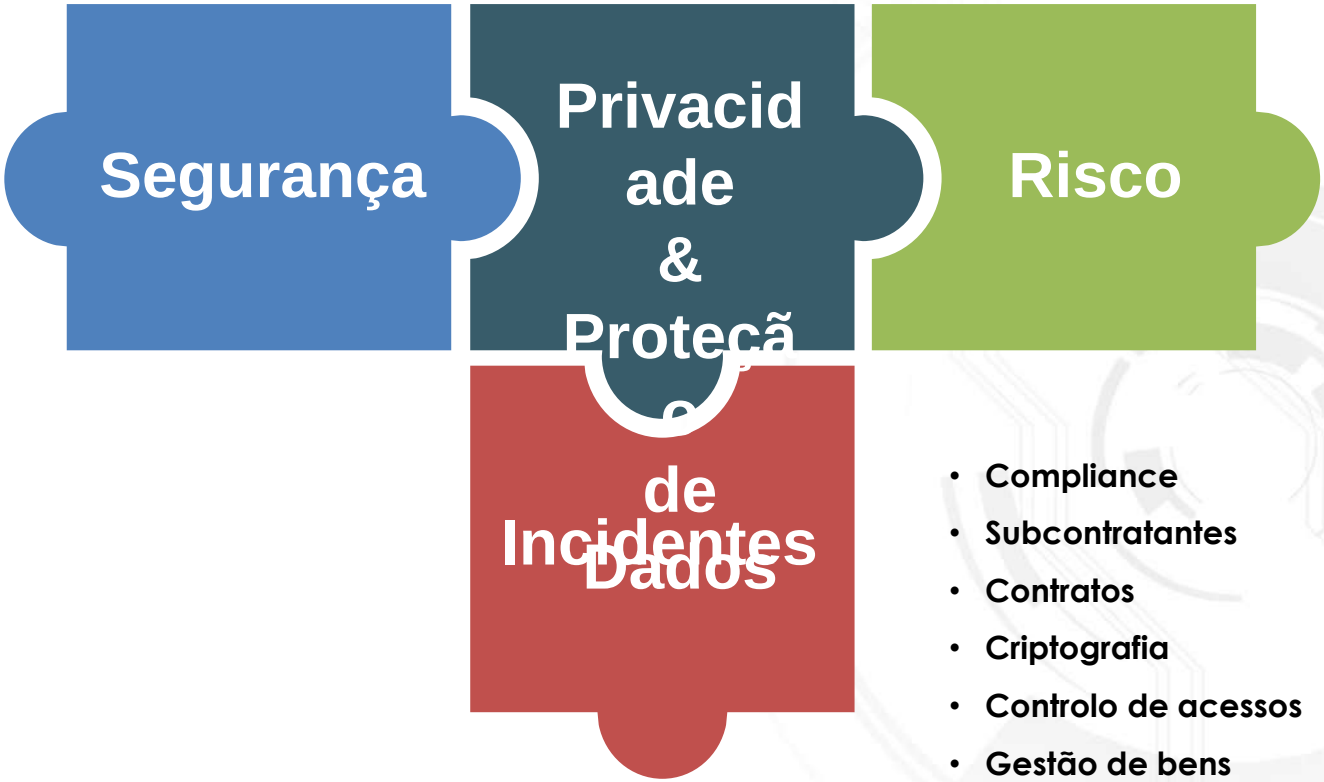
Segurança da Informação & RGPD

24 / 10 / 2018

Nuno Oliveira
Consulting Director & Partner

A ISO 27001 como instrumento para mitigar os riscos da gestão da informação e ferramenta para proteção dos dados pessoais.

Regulamento Geral de Proteção de Dados



- Compliance
- Subcontratantes
- Contratos
- Criptografia
- Controlo de acessos
- Gestão de bens
- Reporting

Segurança

"Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, **adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);** (...)" - Artigo 5.º - 1 f)

"(...) **aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco** (..)" – Artigo 32.º - 1

Preciso de Análise de Risco?

Risco

"Os **riscos deverão ser aferidos** com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado." - Considerando (76)

"(...) **identificação das melhores práticas para a atenuação dos riscos**, (...)" - Considerando (77)

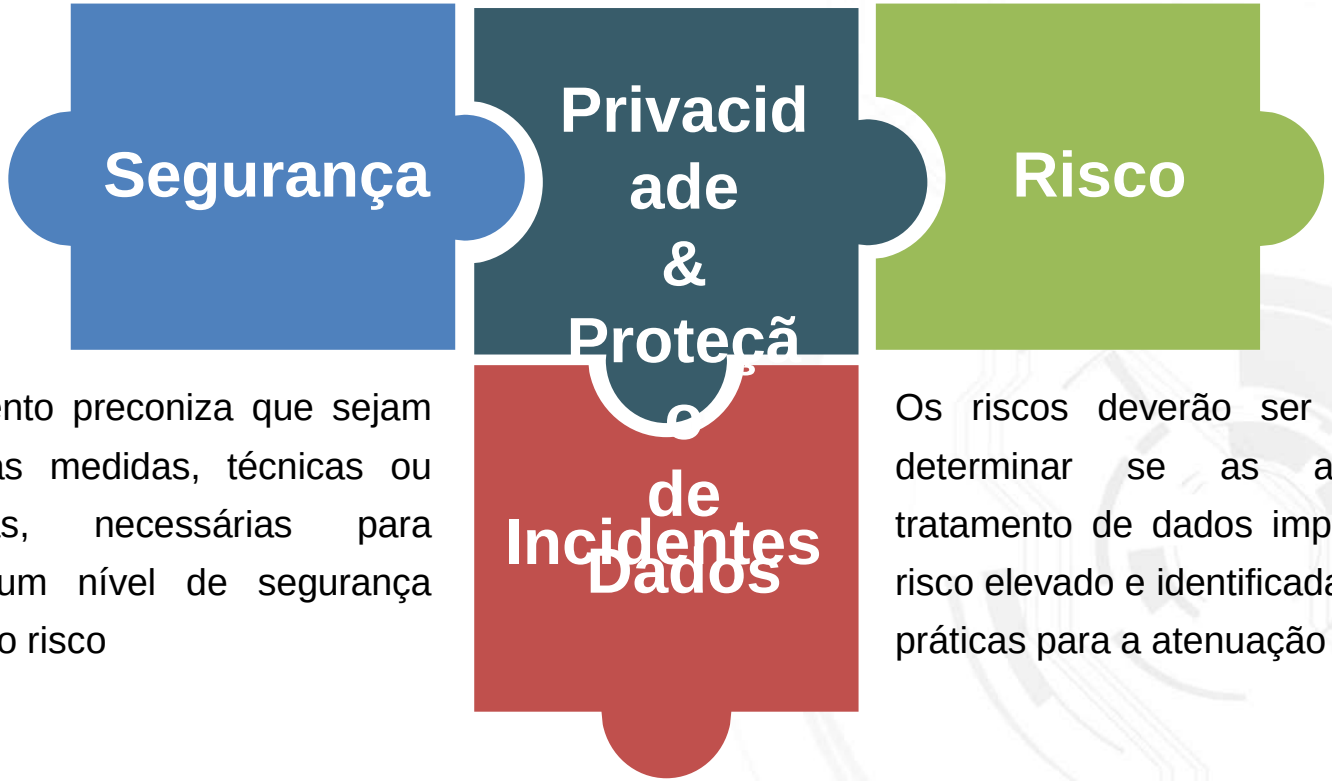
"(...) c) Uma **avaliação dos riscos** para os direitos e liberdades dos titulares dos direitos a que se refere o n.º 1(...)

d) As **medidas previstas para fazer face aos riscos**, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, (...) " – Artigo 35.º

Incidentes

"**Em caso de violação de dados pessoais,** o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, (...)" - Artigo 33.º

"**Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares,** o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada. (…)" - Artigo 34.º



O regulamento preconiza que sejam aplicadas as medidas, técnicas ou organizativas, necessárias para assegurar um nível de segurança adequado ao risco

Os riscos deverão ser aferidos para determinar se as atividades de tratamento de dados implicam risco ou risco elevado e identificadas as melhores práticas para a atenuação desses riscos

Deverá ser garantido que na resposta a incidentes de violação de dados pessoais são geridas as notificações exigidas pelo regulamento

Um sistema de Gestão de Segurança da Informação responde a todos os requisitos do RGPD ?

A implementação e operação de um SGSI permite ...

- ✓ Endereçar 69 dos 99 artigos
  - 30 artigos são diretamente relacionados com a entidade supervisora e processos de *reporting*
- ✓ Adotar uma **gestão de risco** que responde às necessidades do RGPD
- ✓ Adoção de **controlos adequados** para mitigação dos riscos
- ✓ Adoção de uma cultura de **comunicação** e **melhoria continua**
- ✓ **Endereçar os desafios (RGPD) de forma adequada e metodologicamente correta!**

Objetivos: Cumprimento do RGPD, providenciar garantias de controlo de segurança da informação à Organização

Um sistema de Gestão de Segurança da Informação sustenta todas as atividades de operação e gestão de segurança da informação do RGPD. Não endereça contudo os aspetos de índole legal bem como a sua interpretação jurídica.

SISTEMA DA GESTÃO DA PROTEÇÃO DE DADOS

UM NOVO DESAFIO

SÉRGIO FERREIRA – SGS

WHEN YOU NEED TO BE SURE

SGS

- Porque é importante a existência de um Sistema de Gestão de Proteção de Dados Pessoais?

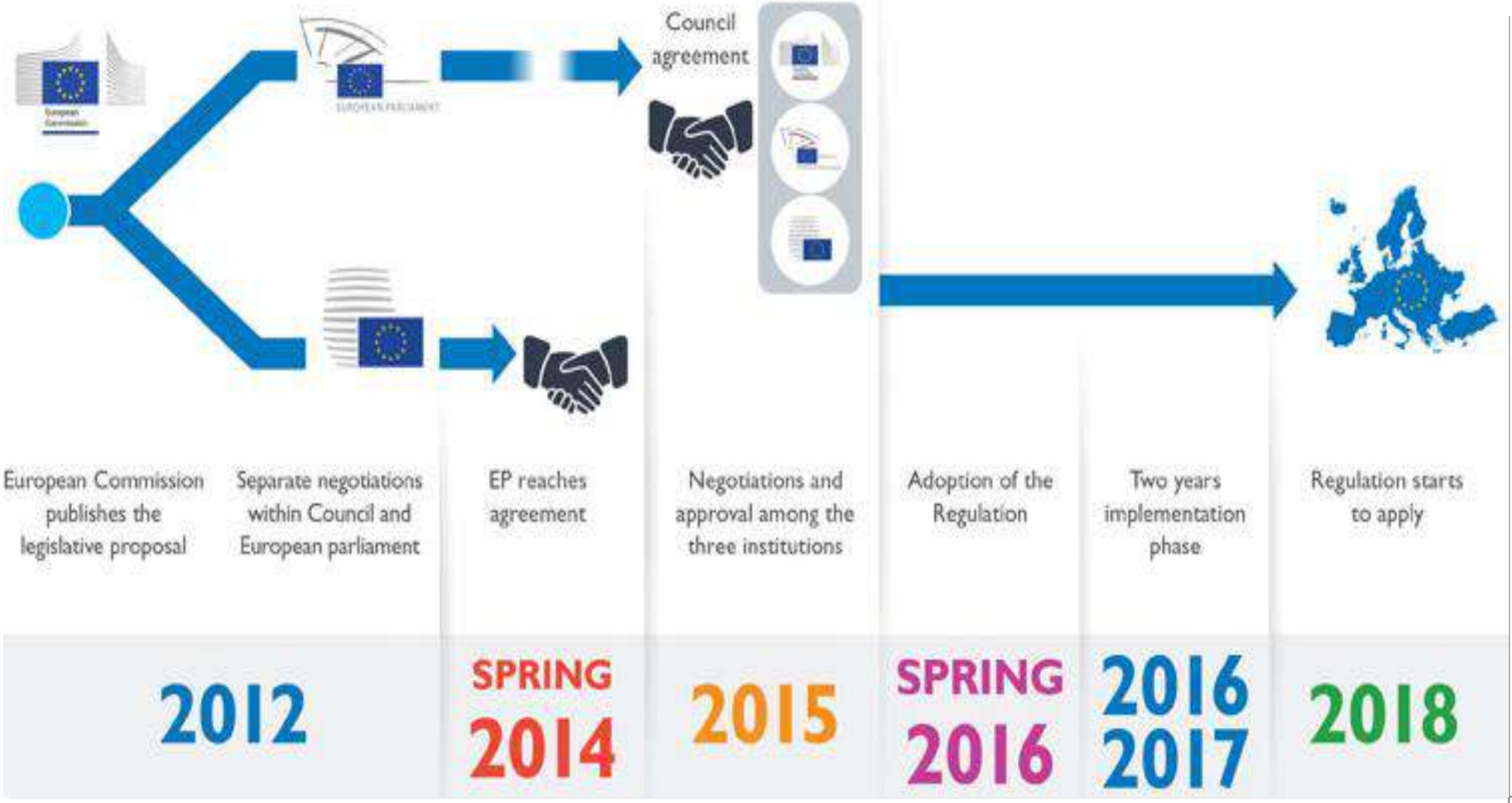
- Qual é o principal catalisador deste sistema?

SISTEMA DE GESTÃO DE PROTEÇÃO DE DADOS PESSOAIS

- REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (RGPD)

- O RGPD regula a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

RGPD TIMELINE



REGULAMENTO GERAL DE PROTEÇÃO DE DADOS
O QUE É?

- Mudança de paradigma na proteção de dados pessoais, onde passamos de uma lógica centrada nas organizações que tratam dados pessoais para uma lógica alinhada com a proteção dos titulares dos dados.

- Essa mudança percebe-se com a inversão do ónus de prova, que antes do RGPD, estava do lado do titular dos dados e que agora passa a estar do lado das organizações.

- De uma forma prática, isto significa que, quem trata dados pessoais, passa a ter a obrigação de provar em que situações é que processou esses dados, para que fim e porquê, quando no passado bastava submeter um pedido de autorização prévia à autoridade competente.

FOCO RGPD: 8 PRINCÍPIO FUNDAMENTAIS

- Livre circulação [arts. 1.º-1, 1.º-3]
- Licitude, lealdade e transparência [art. 5.º-1-a]
- Limitação das finalidades [art. 5.º-1-b]
- Minimização dos dados [art. 5.º-1-c]
- Exactidão [art. 5.º-1-d]
- Limitação da conservação [art. 5.º-1-e]
- Integridade e confidencialidade [art. 5.º-1-f]
- Responsabilidade demonstrada [art. 5.º-2]

- Uma vez que o Regulamento é diretamente aplicável no ordenamento jurídico português, é necessário compreender a complexidade dos diferentes procedimentos e sistemas de gestão e estruturar um plano de ação para a respetiva implementação técnica e operacional, **que garantam a existência de um conjunto de SISTEMAS**

SISTEMA DE GESTÃO DO EXERCÍCIO DOS DIREITOS DOS TITULARES NO ÂMBITO DA PROTECÇÃO DE DADOS

SISTEMA DE REGISTOS DE TRATAMENTO DE DADOS PESSOAIS

SISTEMA DE SEGURANÇA DA INFORMAÇÃO

SISTEMA DE NOTIFICAÇÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

PROPOSTA DE UM SISTEMA DE GESTÃO DE PROTEÇÃO DE DADOS PESSOAIS

SISTEMA DE GESTÃO PARA GARANTIR CUMPRIMENTO COM O RGPD

Diagnóstico → **Implementação** → **Gestão**

- Análise “AS IS”

Diag. → Plan

- Construir plano de Ação para cumprimento do RGPD

Plan → Do

- Implementação do plano

Do → Check

- Verificação e avaliação

Check → Act

- Melhoria:
  Ações corretivas e
  Formação

Act → Plan

Cliente (Org)

OBRIGADO!

www.sgs.pt
pt.info@sgs.com
808 200 747

WHEN YOU NEED TO BE SURE

SGS