



**ISO 27001 – Segurança da Informação –
Vital para a Competitividade da sua
Organização**

DECSIS

Quem Somos?

DECSIS

Apresentação do Grupo
DECSIS

Com origem na *DECSIS, Sistemas de Informação, Lda.*, fundada em 1994, o Grupo DECSIS conta actualmente com mais duas empresas:

- A Decsis II, Redes de Telecomunicações Lda
- A Expandiserve, Sistemas de Informação Lda,

A Missão:



A Missão da **DECSIS** é disponibilizar para os seus Clientes, Produtos e Serviços da mais elevada qualidade dentro da sua área de actuação e de acordo com as suas competências.

Nesse sentido, a **DECSIS** compromete-se com os seus Clientes de que tudo fará tendo em vista atingir e se possível superar as suas expectativas.

Parcerias:

DECSIS



Parcerias:

DECSIS



Parcerias:

DECSIS



Parcerias:

DECSIS



Parcerias:

DECSIS



Parcerias:

DECSIS



A Norma ISO 27001:

DECSIS

Estrutura da Norma
ISO 27001

O que é a ISO 27001?



A norma ISO 27001:2005 é a evolução natural da norma BS7799-2:2002

Um padrão britânico que trata da definição de requisitos para um Sistema Gestão de Segurança da Informação.

O padrão foi incorporado pela *The International Organization for Standardization (ISO)*, Instituição internacional com sede na Suíça que cuida do estabelecimento de padrões internacionais de certificação em diversas áreas.

O Reino Unido tem sido o grande promotor nesta área, pela tradição que tem tido, em actividades de padronização, desde a Revolução Industrial.

ISO 27000

ISO 27001

ISO 27002

ISO 27003

ISO 27004

ISO 27005

ISO 27005

**Vocabulário e definições
a serem utilizadas
pelas restantes Normas**

ISO 27000

ISO 27001

ISO 27002

ISO 27003

ISO 27004

ISO 27005

ISO 27005

**Define os requisitos para
a implementação de
um SGSI**

ISO 27000

ISO 27001

ISO 27002

ISO 27003

ISO 27004

ISO 27005

ISO 27005

**Actual ISO-17799,
Define boas práticas
para a gestão da
segurança da
Informação**

ISO 27000

ISO 27001

ISO 27002

ISO 27003

ISO 27004

ISO 27005

ISO 27005

É um Guia para a
implementação de um
SGSI

ISO 27000

ISO 27001

ISO 27002

ISO 27003

ISO 27004

ISO 27005

ISO 27005

**Define métricas e meios
de medição para
Avaliar a eficácia de um
SGSI**

ISO 27000

ISO 27001

ISO 27002

ISO 27003

ISO 27004

ISO 27005

ISO 27005

**Actual BS 7799-3. Define
linhas de orientação
para a gestão do risco
da segurança da
Informação**

ISO 27000

ISO 27001

ISO 27002

ISO 27003

ISO 27004

ISO 27005

ISO 27005

**Um guia para o processo
de acreditação de
entidades
certificadoras**

A Norma ISO 27001:



Outros Conceitos relacionados com a Norma:
ISO 27001

A **Informação** existe em varias formas. Qualquer que seja a forma que a **Informação** adopte, ou o meio pela qual é partilhada ou armazenada, deve ser sempre devidamente protegida.

A **Informação** é um bem que, à semelhança de outros bens do negócio, tem valor para uma organização e necessita ser convenientemente protegida

A **Informação** existe em varias formas. Qualquer que seja a forma que a **Informação** adopte, ou o meio pela qual é partilhada ou armazenada, deve ser sempre devidamente protegida.

A **Informação** é um bem que, à semelhança de outros bens do negócio, tem valor para uma organização e necessita ser convenientemente protegida

- O **Bem** é algo que tem valor para a organização

- O **Bem** é algo que tem valor para a organização
 - Exemplos:

Pessoas

- O **Bem** é algo que tem valor para a organização
 - Exemplos:

Pessoas

Informação

- O **Bem** é algo que tem valor para a organização
 - Exemplos:

Pessoas

Informação

Produtos

- O **Bem** é algo que tem valor para a organização
- Exemplos:

Pessoas

Informação

Produtos

Edifícios

É a preservação da **Confidencialidade**, **Integridade** e **Disponibilidade** da informação;

- Adicionalmente poderão também ser consideradas, as seguintes propriedades:
 - **Autenticidade**
 - **Responsabilidade**,
 - **Não repudição**
 - **Grau de Confiança/Fiabilidade**

- Vulnerabilidades

Uma fraqueza de um bem ou conjunto de bens, que podem ser explorados por uma ou mais ameaças.

- Ameaças

Uma potencial causa de acidente, que pode resultar em dano ou perda para um sistema ou organização

- Vulnerabilidades

Uma fraqueza de um bem ou conjunto de bens, que podem ser explorados por uma ou mais ameaças.

- Ameaças

Uma potencial causa de acidente, que pode resultar em dano ou perda para um sistema ou organização

Sistema de Gestão da Segurança Informação (SGSI)

É uma parte do sistema global de gestão, baseado numa abordagem de risco, que permite definir, implementar, operacionalizar, monitorizar, manter e melhorar a segurança da Informação segundo a norma.

Que modelo de gestão é utilizado?



O Sistema de gestão SGSI, é baseado numa aproximação sistemática dos riscos inerentes aos negócios,

- Com o objectivo de:
 - Estabelecer
 - Implementar
 - Operar
 - Monitorizar
 - Rever
 - Manter
 - Melhorar a segurança da informação.

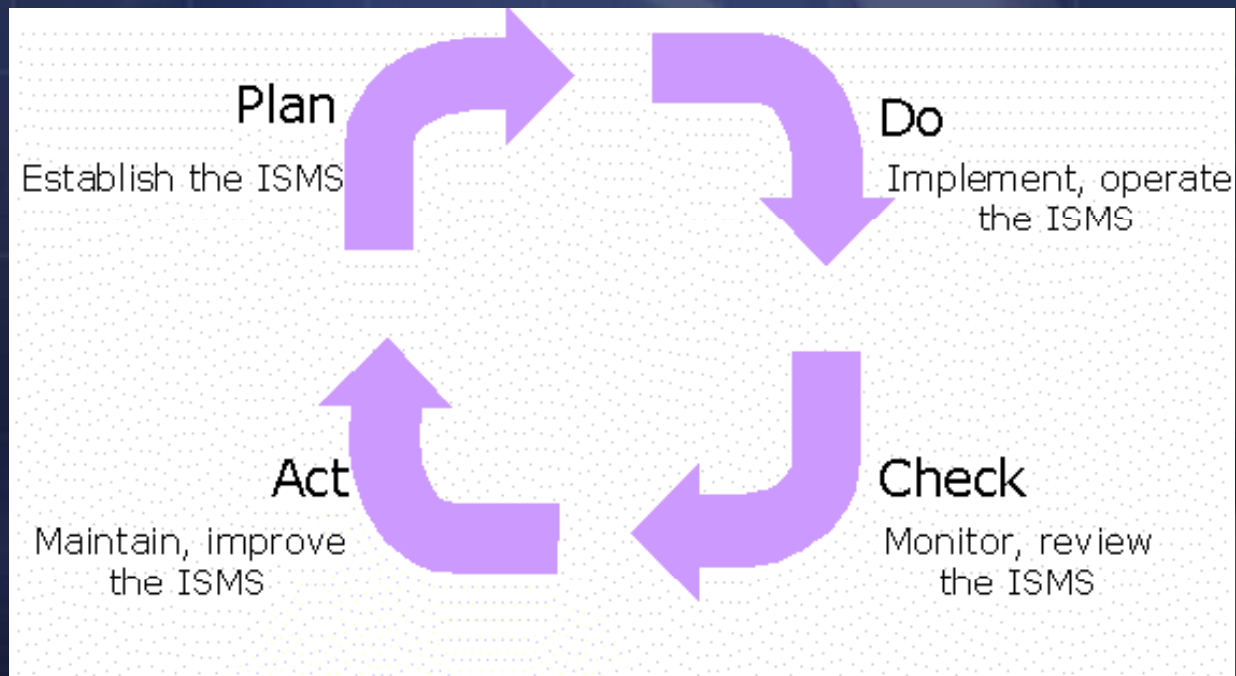
Trata-se de uma abordagem à segurança da informação, numa perspectiva organizacional.

Este sistema denomina-se por

PDCA

Representação do ciclo PDCA?

Requisitos
Expectativas



Segurança da
Informação
Gerida

- Requisitos Gerais do SGSI:
 - Deve-se
 - Desenvolver, implementar, manter e melhorar continuamente o SGSI
 - Definir políticas e objectivos
 - Estabelecer o ciclo PDCA
- Definir o SGSI
 - Deve-se:
 - Definir o âmbito, política, abordagem sistemática para avaliação do risco
 - Identificar e avaliar alternativas para tratamento dos riscos
 - Obter aprovação, da gestão de topo, para os riscos residuais
 - Preparar a matriz de controlos já composta por 133 controlos (*Statment of Application*)

- Requisitos Gerais do SGSI:
 - Deve-se
 - Desenvolver, implementar, manter e melhorar continuamente o SGSI
 - Definir políticas e objectivos
 - Estabelecer o ciclo PDCA
- Definir o SGSI
 - Deve-se:
 - Definir o âmbito, a política, e a abordagem sistemática para avaliação do risco
 - Identificar e avaliar alternativas para tratamento dos riscos
 - Obter aprovação, da gestão de topo, para os riscos residuais
 - Preparar a matriz de controlos já composta por 133 controlos (*Statment of Application*)

- Como implementar e operacionalizar o SGSI?
 - Deve-se:
 - Definir um plano de tratamentos de risco que identifique as actividades de gestão apropriadas, recursos, responsabilidades e prioridades para gerir os riscos à segurança da Informação.
 - Definir como medir a eficácia dos controlos
 - Implementar programas de formação e sensibilização
 - Gerir a componente operacional do SGSI
 - Implementar procedimentos e outros controlos capazes de detectarem e responderem a potenciais incidentes na segurança

- Como monitorizar e rever o SGSI:
 - Devem-se:
 - Executar procedimentos de monitorização
 - Rever a eficácia do SGSI
 - Rever os níveis de risco residual
 - Realizar auditorias internas periodicamente
 - Realizar revisões com a gestão de topo – para garantir o âmbito do SGSI e identificação de melhorias
 - Actualizar planos de segurança

- Como manter e melhorar o SGSI:
 - Deve-se:
 - Implementar as melhorias identificadas no SGSI
 - Implementar as acções correctivas e preventivas
 - Comunicar os resultados e acções
 - Garantir que as melhorias atingem os objectivos pretendidos.

- Como em qualquer SGSI:
 - Deve existir documentação sobre:
 - Todos os, procedimentos, controlos, políticas e objectivos definidos
 - O Âmbito do SGSI
 - Metodologias de avaliação do risco
 - Relatórios de avaliação e planos de tratamento do risco

Documentação de todos os procedimentos necessários á organização, afim de garantir a eficiência do seu planeamento, operacionalidade e controlo dos processos de segurança da informação.

- **Fase 1 - Definição do âmbito e da política**
- **Fase 2 - Identificação dos Bens**
- **Fase 3 - Valorização dos Bens**
- **Fase 4 - Identificação do Risco**
- **Fase 5 - Identificação dos controlos e Risco Residual**
- **Fase 6 - Aceitação do Risco Residual e Identificação de Políticas**
- **Fase 7 - Definição de Políticas e Processos para implementação dos controlos**
- **Fase 8 - Implementação de Políticas e processos**
- **Fase 9 - Elaboração da documentação**
- **Fase 10 - Auditoria e revisão do SGSI**

- **Fase 1 - Definição do âmbito e da política**
- **Fase 2 - Identificação dos Bens**
- **Fase 3 - Valorização dos Bens**
- **Fase 4 - Identificação do Risco**
- **Fase 5 - Identificação dos controlos e Risco Residual**
- **Fase 6 - Aceitação do Risco Residual e Identificação de Políticas**
- **Fase 7 - Definição de Políticas e Processos para implementação dos controlos**
- **Fase 8 - Implementação de Políticas e processos**
- **Fase 9 - Elaboração da documentação**
- **Fase 10 - Auditoria e revisão do SGSI**

- **Fase 1 - Definição do âmbito e da política**
- **Fase 2 - Identificação dos Bens**
- **Fase 3 - Valorização dos Bens**
- **Fase 4 - Identificação do Risco**
- **Fase 5 - Identificação dos controles e Risco Residual**
- **Fase 6 - Aceitação do Risco Residual e Identificação de Políticas**
- **Fase 7 - Definição de Políticas e Processos para implementação dos controles**
- **Fase 8 - Implementação de Políticas e processos**
- **Fase 9 - Elaboração da documentação**
- **Fase 10 - Auditoria e revisão do SGSI**

- **Fase 1 - Definição do âmbito e da política**
- **Fase 2 - Identificação dos Bens**
- **Fase 3 - Valorização dos Bens**
- **Fase 4 - Identificação do Risco**
- **Fase 5 - Identificação dos controles e Risco Residual**
- **Fase 6 - Aceitação do Risco Residual e Identificação de Políticas**
- **Fase 7 - Definição de Políticas e Processos para implementação dos controles**
- **Fase 8 - Implementação de Políticas e processos**
- **Fase 9 - Elaboração da documentação**
- **Fase 10 - Auditoria e revisão do SGSI**

- **Fase 1 - Definição do âmbito e da política**
- **Fase 2 - Identificação dos Bens**
- **Fase 3 - Valorização dos Bens**
- **Fase 4 - Identificação do Risco**
- **Fase 5 - Identificação dos controlos e Risco Residual**
- **Fase 6 - Aceitação do Risco Residual e Identificação de Políticas**
- **Fase 7 - Definição de Políticas e Processos para implementação dos controlos**
- **Fase 8 - Implementação de Políticas e processos**
- **Fase 9 - Elaboração da documentação**
- **Fase 10 - Auditoria e revisão do SGSI**

- **Fase 1 - Definição do âmbito e da política**
- **Fase 2 - Identificação dos Bens**
- **Fase 3 - Valorização dos Bens**
- **Fase 4 - Identificação do Risco**
- **Fase 5 - Identificação dos controlos e Risco Residual**
- **Fase 6 - Aceitação do Risco Residual e Identificação de Políticas**
- **Fase 7 - Definição de Políticas e Processos para implementação dos controlos**
- **Fase 8 - Implementação de Políticas e processos**
- **Fase 9 - Elaboração da documentação**
- **Fase 10 - Auditoria e revisão do SGSI**

- **Fase 1 - Definição do âmbito e da política**
- **Fase 2 - Identificação dos Bens**
- **Fase 3 - Valorização dos Bens**
- **Fase 4 - Identificação do Risco**
- **Fase 5 - Identificação dos controlos e Risco Residual**
- **Fase 6 - Aceitação do Risco Residual e Identificação de Políticas**
- **Fase 7 - Definição de Políticas e Processos para implementação dos controlos**
- **Fase 8 - Implementação de Políticas e processos**
- **Fase 9 - Elaboração da documentação**
- **Fase 10 - Auditoria e revisão do SGSI**

- **Fase 1 - Definição do âmbito e da política**
- **Fase 2 - Identificação dos Bens**
- **Fase 3 - Valorização dos Bens**
- **Fase 4 - Identificação do Risco**
- **Fase 5 - Identificação dos controlos e Risco Residual**
- **Fase 6 - Aceitação do Risco Residual e Identificação de Políticas**
- **Fase 7 - Definição de Políticas e Processos para implementação dos controlos**
- **Fase 8 - Implementação de Políticas e Processos**
- **Fase 9 - Elaboração da documentação**
- **Fase 10 - Auditoria e revisão do SGSI**

- **Fase 1 - Definição do âmbito e da política**
- **Fase 2 - Identificação dos Bens**
- **Fase 3 - Valorização dos Bens**
- **Fase 4 - Identificação do Risco**
- **Fase 5 - Identificação dos controlos e Risco Residual**
- **Fase 6 - Aceitação do Risco Residual e Identificação de Políticas**
- **Fase 7 - Definição de Políticas e Processos para implementação dos controlos**
- **Fase 8 - Implementação de Políticas e processos**
- **Fase 9 - Elaboração da documentação**
- **Fase 10 - Auditoria e revisão do SGSI**

- **Fase 1 - Definição do âmbito e da política**
- **Fase 2 - Identificação dos Bens**
- **Fase 3 - Valorização dos Bens**
- **Fase 4 - Identificação do Risco**
- **Fase 5 - Identificação dos controlos e Risco Residual**
- **Fase 6 - Aceitação do Risco Residual e Identificação de Políticas**
- **Fase 7 - Definição de Políticas e Processos para implementação dos controlos**
- **Fase 8 - Implementação de Políticas e processos**
- **Fase 9 - Elaboração da documentação**
- **Fase 10 - Auditoria e revisão do SGSI**

A Segurança da Informação é um problema Organizacional e não tecnológico

A implementação de segurança tem que ser um compromisso entre o risco, o grau de protecção desejado e o custo do mecanismo de controlo.

O Caminho para a segurança da Informação é a gestão do risco através da integração das componentes de... Gestão e Tecnologia

A Segurança da Informação é um problema Organizacional e não tecnológico

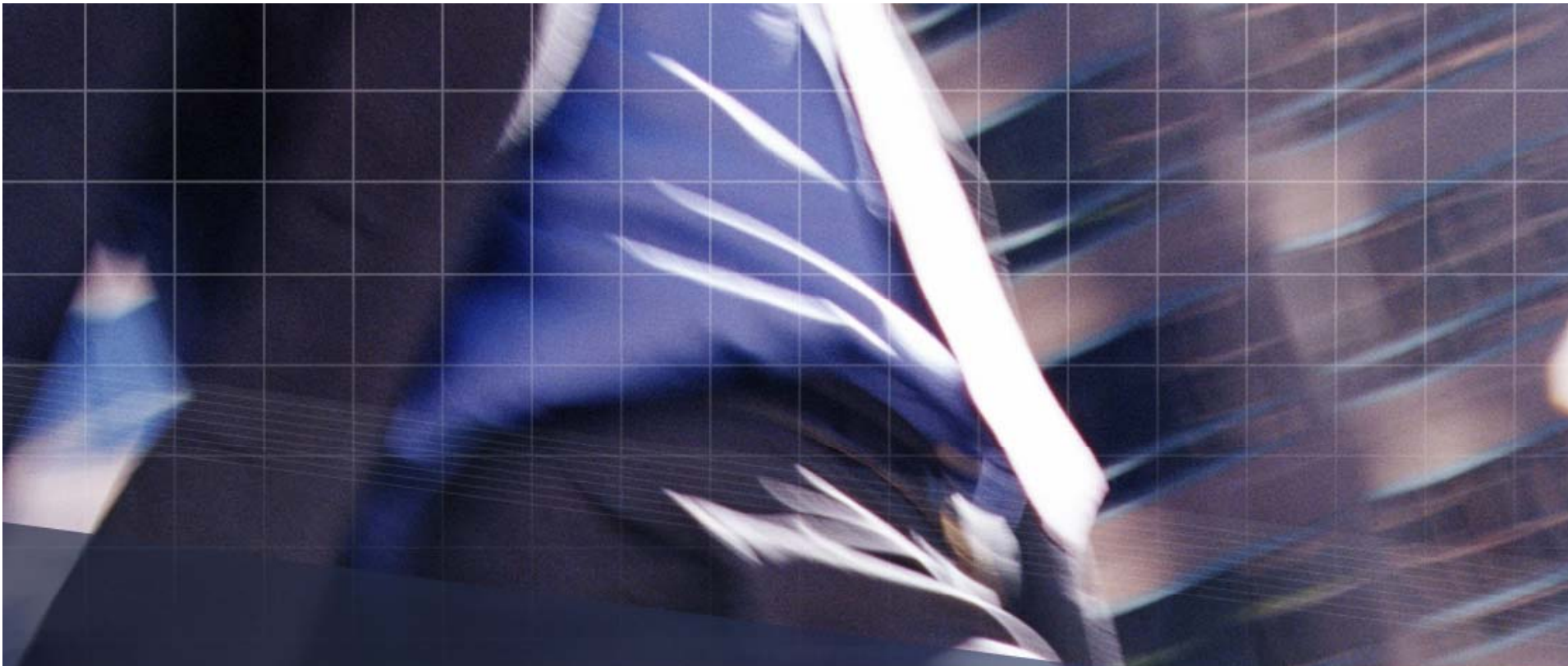
A implementação de segurança tem que ser um compromisso entre o risco, o grau de protecção desejado e o custo do mecanismo de controlo.

O Caminho para a segurança da Informação é a gestão do risco através da integração das componentes de... Gestão e Tecnologia

A Segurança da Informação é um problema Organizacional e não tecnológico

A implementação de segurança tem que ser um compromisso entre o risco, o grau de protecção desejado e o custo do mecanismo de controlo.

O Caminho para a segurança da Informação é a gestão do risco através da integração das componentes de.... **Gestão e Tecnologia**



DECSIS SI

António Pedro Martins

Tel.: +351 962032835

mailto: antonio.martins@decsis.pt

DECSIS