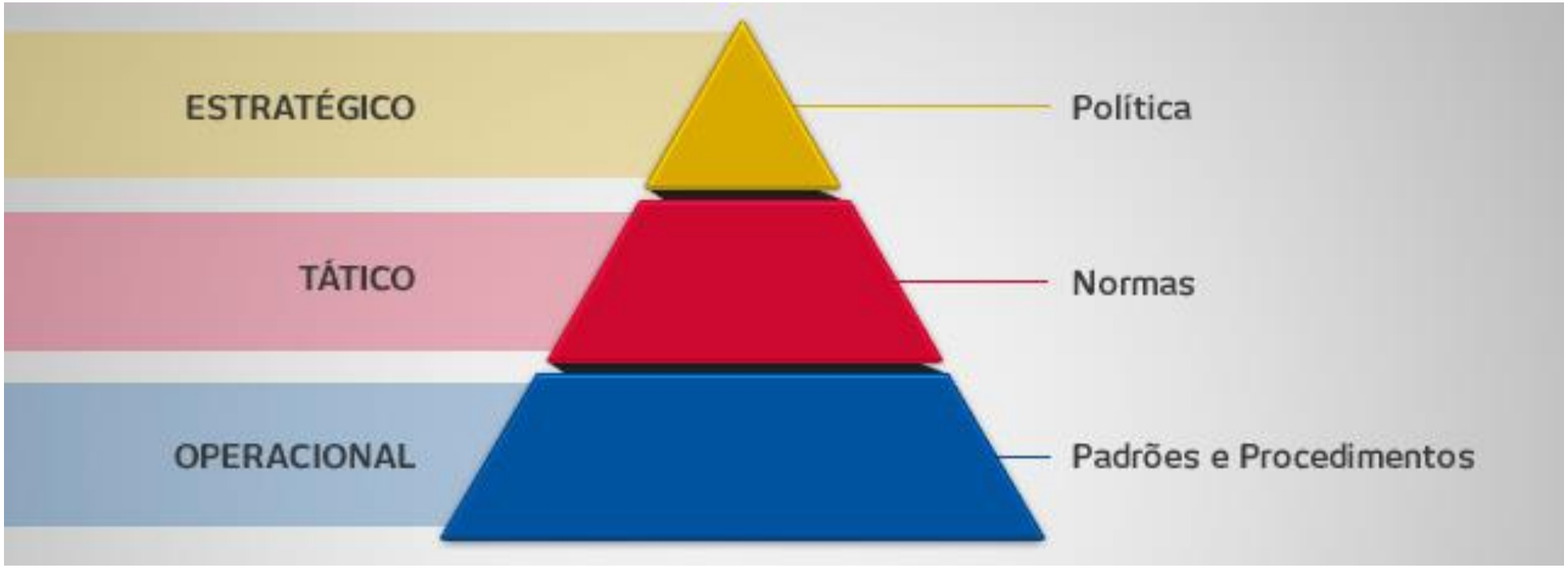
Normas da Segurança da Informação



Normas da Segurança da Informação

Unidade 6 - Normas da Segurança da Informação

- 6.1 - O que é a Norma ISO 27001 e 27002
- 6.2 - Para que serve
- 6.3 - Quais os benefícios para quem adota
- 6.4 - Pontos abordados pelas normas
- 6.5 - Pequeno projeto para aplicação da normas

Normas da Segurança da Informação

- ISO - “International Organization for Standardization” é uma organização sediada em Genebra, na Suiça. Foi fundada em 1946. O propósito da ISO é desenvolver e promover normas que possam ser utilizadas igualmente por todos os países do mundo.

Normas da Segurança da Informação

- Em todas as empresas, fazer uma gestão da informação eficiente garante benefícios que vão da proteção de dados estratégicos à obtenção de novos negócios.
- Para que a companhia possa usufruir do que uma gestão adequada oferece, é preciso garantir que políticas, processos, *hardwares* e *softwares* supram suas necessidades, considerando todos os riscos e atividades do negócio.
- Uma maneira de ter certeza de que está tudo sendo feito corretamente é seguir orientações de normas de segurança da informação, que determinam controles, regras e diretrizes para a área.

Normas da Segurança da Informação

- A equipe de Tecnologia da Informação pode usar como guia de boas práticas as recomendações das normas ISO/IEC da série 27000.
- Elas abordam Sistema de Gestão de Segurança da Informação (SGSI), gestão de riscos, aplicação de controles, monitoramento, revisões e outros aspectos.
- São uma maneira de implementar, monitorar e estabelecer objetivos tangíveis.

Normas da Segurança da Informação

- **O que são normas técnicas**
- As normas técnicas determinam regras, diretrizes e características mínimas para atividades ou resultados.
- Elas são aprovadas por um organismo reconhecido e as empresas que atendem suas exigências podem receber uma comprovação de excelência quando auditadas.
- Em muitos casos, clientes exigem que as companhias possuam determinadas certificações para fecharem negócios, já que assim eles garantem que serviços e produtos são oferecidos de acordo com boas práticas internacionais, que podem ser de gestão, segurança, inovação ou processo.

Normas da Segurança da Informação

- **O que são normas técnicas (continuação)**
- Para as instituições serem certificadas, elas passam por auditorias realizadas por entidades certificadoras, que checam todos os processos e conformidades.
- O processo de obtenção do certificado pode variar de acordo com o serviço, produto ou o porte da companhia, mas geralmente inclui aplicação das diretrizes da norma, análise de documentação, realização de auditorias internas para verificação de inconformidades, adequação e auditorias externas.

Normas da Segurança da Informação

- **Normas de segurança da informação**
- Existem normas que regem a elaboração e aplicação de um Sistema de Gestão de Segurança da Informação.
- Elas têm o objetivo de garantir confidencialidade, integridade e disponibilidades da informação, fatores essenciais para um sistema corporativo seguro.

Normas da Segurança da Informação

- **Evolução**
- A BS7799, norma britânica desenvolvida pelo British Standards Institution, é amplamente conhecida.
- Ela foi aprovada pela ISO (International Organization for Standardization) e pela IEC (International Electrotechnical Commission) para utilização internacional e passou a ser conhecida como ISO/IEC 17799 em 2000.
- A partir de 2005, começaram a ser publicadas as normas da série 27000, como a ISO/IEC 27002, que substituiu a 17799.

Normas da Segurança da Informação

- **Vantagens**
- A aplicação das normas da série ISO/IEC 27000 não é obrigatória, mas elas reúnem recomendações para uma gestão eficiente e que entregue bons resultados para a companhia. Dentre elas, apenas a 27001 é passível de certificação. As demais funcionam como base para alcançar os resultados positivos.
- A ISO/IEC 27001 define requisitos para implementação, operação, monitoramento, revisão, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação. Ela pode ser aplicada em qualquer organização, independentemente de porte ou setor e é ainda mais valorizada em empresas que priorizam a segurança da informação e a têm como fator crítico para as operações, como é o caso de empresas de finanças, TI e setores públicos.

Normas da Segurança da Informação

- **Vantagens (Continuação)**
- Embora essa certificação não seja obrigatória, ela pode trazer diversos benefícios para a sua companhia:
  - Maior segurança para a rede corporativa
  - Diferencial para clientes que buscam empresas parceiras certificadas
  - Redução de custos com prevenção de incidentes de segurança da informação
  - Mais organização e produtividade
  - Conformidade com requisitos legais
  - Valor de mercado para divulgações e diferenciação em negociações

6.1-O que é a Norma ISO 27001 e 27002

- A ISO/IEC 27001 e a ISO 27002 são normas internacionais publicadas pela Standardization Organization (ISO) e pela International Electrotechnical Commission (IEC).
- Elas definem, respectivamente, os requisitos e as melhores práticas para o Sistema de Gestão de Segurança da Informação (SGSI).

6.1-O que é a Norma ISO 27001 e 27002

- Enquanto as empresas podem ser certificadas pela ISO/IEC 27001, a 27002 funciona como um guia de práticas e controles que facilitam o alcance da primeira e pode ser usada em pequenas, médias e grandes companhias de todos os setores.
- Empresas que aplicam as orientações dessas normas garantem um SGSI conforme orientações internacionais e usufruem de seus benefícios, entre eles redução de riscos e melhor organização de processos.

6.1-O que é a Norma ISO 27001 e 27002

- **Série ISO 27000**
- As 45 normas desta família são projetadas com focos diferentes dentro da Segurança da Informação.
- Elas podem ser para implementação do SGSI, controles, métricas, avaliação e tratamento de riscos, auditoria, gestão e muitos outros objetivos.
- Dentre elas, apenas a ISO 27001 é auditável e os profissionais somente podem ser certificados na ISO 27002.

6.2-Para que serve

- **ISO 27001**
- Essa é uma norma de gestão que define os requisitos para a sua empresa possuir e administrar um Sistema de Gestão de Segurança da Informação certificado.
- Ela leva em consideração os ativos da companhia e as necessidades da área de negócio para definir a melhor forma de administrar o sistema.
- Em suma, isso significa que a segurança da informação deve ser planejada, implementada, monitorada, analisada e melhorada para seu nicho de trabalho. Com isso, todas as responsabilidades são definidas e os objetivos estabelecidos, medidos, analisados e auditados internamente.

6.2-Para que serve

- **ISO 27002**
- Essa norma era o antigo padrão 17799:2005. Ela estabelece um código de melhores práticas para apoiar a implantação do Sistema de Gestão de Segurança da Informação (SGSI) nas organizações e tem como objetivo estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.
- A ISO/IEC 27002 funciona como um guia completo de implementação, em que descreve como quais controles devem ser estabelecidos e de que forma. Ela tem como base uma avaliação de riscos dos ativos mais importantes da empresa.
- Ela não deve ser utilizada em auditorias mas simplesmente servir como um guia.

6.1-O que é a Norma ISO 27001 e 27002

- **ISO 27002**
- É preciso lembrar que, em sua empresa, a tecnologia, as pessoas, a gestão, os processos, a segurança e os negócios estão interligados e é necessário saber lidar com a informação para garantir integridade, confidencialidade e disponibilidade.

6.1-O que é a Norma ISO 27001 e 27002

- **ISO 27002**
- Mesmo que a sua empresa não tenha interesse em ser auditada na norma ISO 27001, seguir as boas práticas da ISO 27002 pode ajudá-la a alcançar um Sistema de Gestão de Segurança da Informação mais robusto.
- Ao seguir suas orientações, você garantirá que a equipe (e os demais funcionários da companhia) tenha maior conscientização sobre a segurança da informação, fator fundamental para que seus dados não sejam acessados por terceiros não autorizados.

6.3-Quais os benefícios para quem adota

- **ISO 27001**
- Entre seus benefícios, estão:
  - Redução de risco de responsabilidade pela não implementação ou determinação de políticas e procedimentos
  - Oportunidade de identificar e corrigir pontos fracos
  - A segurança da informação passa a ser responsabilidade da alta gestão da companhia
  - Permite revisão independente do sistema de gestão da segurança da informação
  - Garante maior confiabilidade aos parceiros e clientes
  - Aumenta a conscientização interna sobre segurança
  - Combina recursos com outros Sistemas de Gestão
  - Permite medir o sucesso do sistema

6.3-Quais os benefícios para quem adota

- **ISO 27002**
- Além disso, são vários os benefícios da aplicação da norma:
  - Maior controle de ativos e informações estratégicas
  - Identificação e correção de pontos fracos do Sistema
  - Diferencial competitivo para clientes que valorizam a conformidade com normas internacionais
  - Melhor organização dos processos
  - Redução de custos com a prevenção de incidentes de segurança da informação
  - Conformidade com a legislação e outras regulamentações.

6.4-Pontos abordados pelas normas

- Entender a organização, o e seu contexto, analisando questões internas e externas relevantes para o seu propósito e os resultados pretendidos com o SGSI;
- Entender necessidades e expectativas das partes interessadas; e
- Determinar o escopo do SGSI, definindo limites e a aplicabilidade do mesmo.

6.4-Pontos abordados pelas normas

- Assegurar que o SGSI possa alcançar seus resultados;
- Prevenir ou reduzir os efeitos indesejados;
- Alcançar a melhoria contínua.
- Ações para considerar os riscos e oportunidades;
- Integrar e implementar essas ações nos processos do seu SGSI;
- Avaliar a eficácia destas ações;

6.4-Pontos abordados pelas normas

- Estabelecer e manter critérios de aceitação do risco;
- Assegurar que as contínuas avaliações de riscos de Segurança da Informação produzam resultados comparáveis, válidos e consistentes;
- Identificar os riscos de Segurança da Informação (utilizando o processo de avaliação do risco, inclusive identificando responsáveis);
- Analisar os riscos de Segurança da Informação (consequências e probabilidades);
- Avaliar os riscos de Segurança da Informação (comparando resultados e priorizando os riscos).

6.5-Pequeno projeto para aplicação da normas

Passos para executar para obter a certificação ISO 27001:

- **1. Obter o apoio da gerência**
- **2. Tratar como um projeto**
- **3. Definir o escopo**
- **4. Escrever uma política do SGSI**
- **5. Definir a metodologia da avaliação de riscos**
- **6. Realizar avaliação de riscos e tratamento de riscos**

6.5-Pequeno projeto para aplicação da normas

Passos para executar para obter a certificação ISO 27001:

- **1. Obter o apoio da gerência**
- **2. Tratar como um projeto**
- **3. Definir o escopo**
- **4. Escrever uma política do SGSI**
- **5. Definir a metodologia da avaliação de riscos**
- **6. Realizar avaliação de riscos e tratamento de riscos**
- **7. Escrever a Declaração de aplicabilidade**
- **8. Elaborar o Plano de tratamento de riscos**

6.5-Pequeno projeto para aplicação da normas

- Passos para executar para obter a certificação ISO 27001:
- **9. Definir como medir a eficiência dos controles**
- **10. Implementar os controles e procedimentos obrigatórios**
- **11. Implementar programas de treinamento e conscientização**
- **12. Operar o SGSI**
- **13. Monitorar o SGSI**
- **14. Realizar auditoria interna**
- **15. Executar análise crítica da gestão**
- **16. Ações corretivas e preventivas**