INSTITUTO FEDERAL
Farroupilha

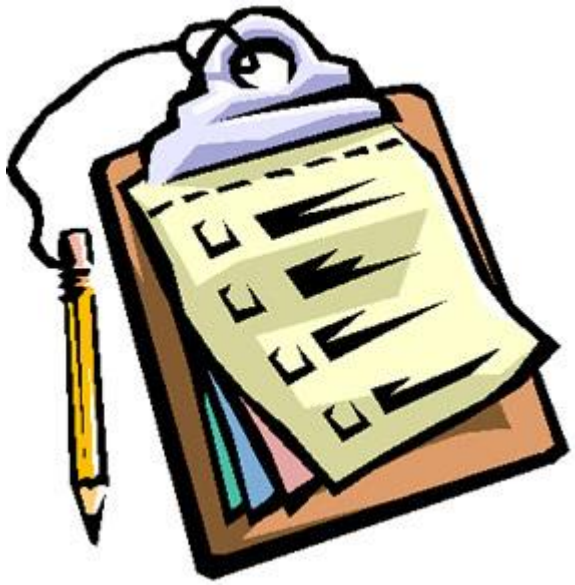
Fonte: http://www.ezequieljuliano.com.br/wp-content/uploads/2014/09/iso27001.jpg

Gestão da Segurança da Informação e Normas

Prof. Gleizer Bierhalz Voss

Roteiro

- Revisão da última aula
- Gestão da Segurança da Informação e Normas
  - Norma 27001;
  - Norma 27002;
  - Norma 27003;
  - Norma 27004;
  - Norma 27006;
  - Norma 27014;
  - Norma 27031;
  - Norma 27040;
  - Políticas de Segurança



Última aula...

- Revisão da Última Aula;
  - BS 7799
  - ISO/IEC 17799
  - ISO 13335
  - ISO/IEC 27000

Questionamento / Objetivo

- Norma 27000
  - O que são?
  - De onde vem?
  - Como se formam?
  - O que fazem?

- Proporcionar a construção de saberes aos alunos com a apresentação dos principais conceitos, relações e componentes envolvidos no emprego de Normativas de Segurança da Informação.

Caso Real

- A CommCorp é um dos maiores provedores de serviços da área de data center e telecomunicações no Rio Grande do Sul e sua infraestrutura ocupa vários andares do SulAmérica;
- Afetou diversos setores;

Caso Real

- Empresa BRDigital – Grupo Commcorp

BRDigital atingida por incêndio

Maurício Renner
// quarta, 07/03/2018 09:43

E-mail | Twittar | Curtir 116 | Compartilhar

A BRDigital teve um dos seus data centers atingido por um princípio de incêndio nesta terça-feira, 06, em Porto Alegre.

Data center fica no centro de Porto Alegre. Foto: Jonathas Costa.

- **AWS derruba Mercado Livre**
- **Problema elétrico derruba Santander**
- **Chile e Argentina disputam DC da AWS**

Os bombeiros foram chamados e evacuaram e desligaram a eletricidade de todo o edifício Sul América, um prédio de 13 andares ao lado da Praça da Alfândega, no coração da capital gaúcha.

Não houve feridos, mas alguns clientes da BRDigital sofreram indisponibilidade de serviços, segundo a companhia informou em comunicado.

Um dos clientes afetados foi a Unimed Porto Alegre, que comunicou indisponibilidade de serviços no Facebook.

O incêndio foi logo controlado, mas a Polícia Civil interditou o prédio para perícia, agendada para esta quarta, 07.

Notícias >> Geral 06/03/2018 | 16:11 | Atualização: 17:19

Bombeiros combatem incêndio no Centro de Porto Alegre

Alguns prédios localizados na General Câmara e Sete de Setembro foram evacuados

Prédios foram evacuados no entorno da General Câmara com a Sete de Setembro | Foto: Jonathas Costa /

Caso Real

- Empresa BRDigital – Grupo Commcorp

Caso Real

- Microsoft

Uma falha no sistema de extintores de incêndio deixou a nuvem Azure da Microsoft fora do ar por sete horas em parte da Europa no final de setembro.

Acionamento acidental de extintores causou falha. Foto: Pixabay.

- **Microsoft: primeira nuvem na África**
- **AWS contrata criador do Java**
- **CIO troca IBM por AWS e leva processo**

Segundo **relata** o site The Register, máquinas virtuais, serviços de cloud, backup, Azure Cache, Azure Monitor, Azure Functions e uma série de outras funcionalidades foram afetadas no dia 29 de setembro.

Os problemas foram causados por funcionários executando uma manutenção de rotina no sistema de extintores de incêndio, que acabou sendo acionado acidentalmente.

A entrada em funcionamento desse sistema, que usa gás, ativa por tabela o desligamento do ar condicionado, para evitar que o fogo se espalhe pelos condutos. Sem ar, algumas máquinas desligaram ou se reiniciaram, fazendo cair uma "storage scale unit".

De acordo com **nota técnica** da Microsoft, o ar voltou em 35 minutos, mas alguns dos servidores e sistemas de storage que superaqueceram demoraram mais para voltar ao ar, fazendo com que máquinas virtuais fossem desligadas para evitar problemas com os dados.

Norma 27000

- Norma essencial para quem está iniciando na área de Segurança da Informação;
- Abrange muitos aspectos atuais e importantes;
- Ajuda muito nas certificações;
- Diferentes versões;
- Base para a disciplina.

Norma 27001

- Padrão de referência internacional para gestão da segurança da informação;
- Milhares de profissionais vêm contribuindo para seu amadurecimento;
- Milhares de instituições se baseiam nela;

Norma 27001

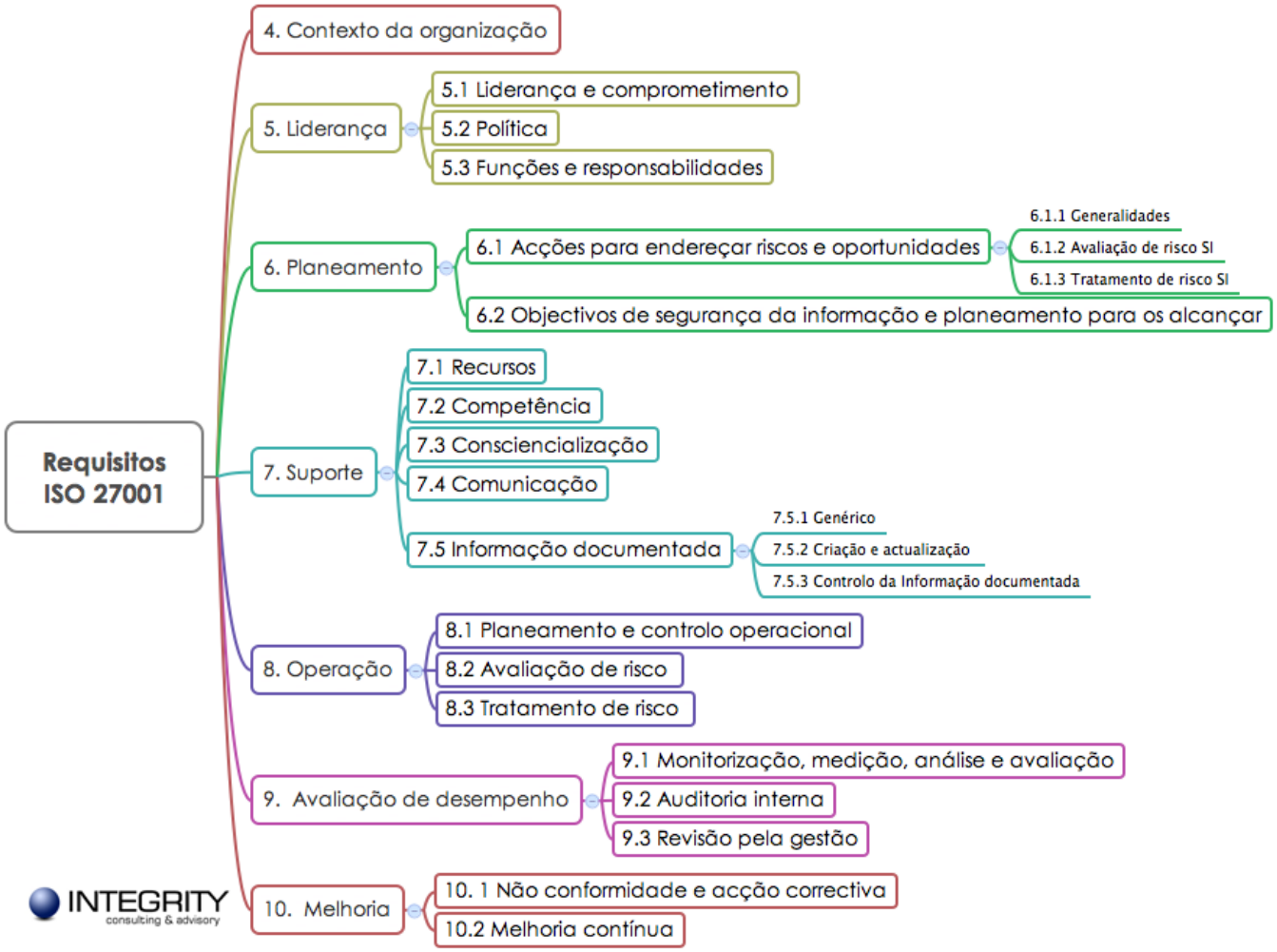
- Adoção de um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um Sistema de Gestão de Segurança da Informação;
- Evolução da BS 7799.

Norma 27001

- A norma padrão (Standard) ISO 27001 é composta por dois componentes relativamente distintos:
  - O primeiro componente, é onde são definidas as regras e os requisitos de cumprimento da norma;
  - O segundo componente da norma, é denominada de ANEXO A e é na realidade composta por um conjunto de controles que as organizações devem adoptar, em diferentes temas

Norma 27001

- Esquema;



Fonte: https://www.27001.pt/iso27001_3.html

Norma 27001

- Esquema;

Fonte: https://www.27001.pt/iso27001_3.html

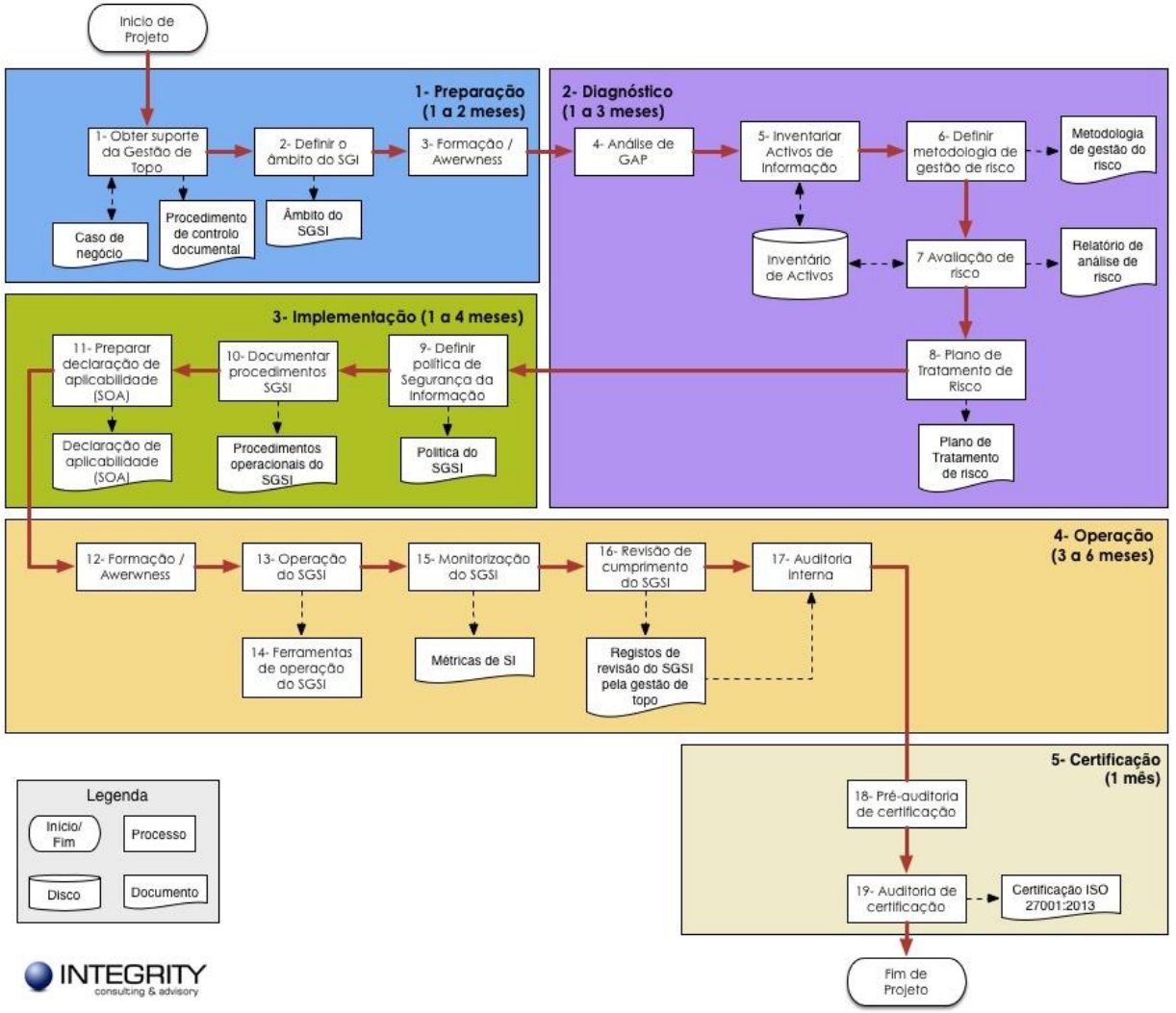
Norma 27001

Benefícios

- Compromisso da organização com SI;
- Confiabilidade e segurança dos sistemas;
- Investimentos conscientes e menores riscos;
- Organização da segurança;
- Confiança e satisfação dos clientes;
- Implementação dos controles;
- Sistema de controle de gestão.

Norma 27001

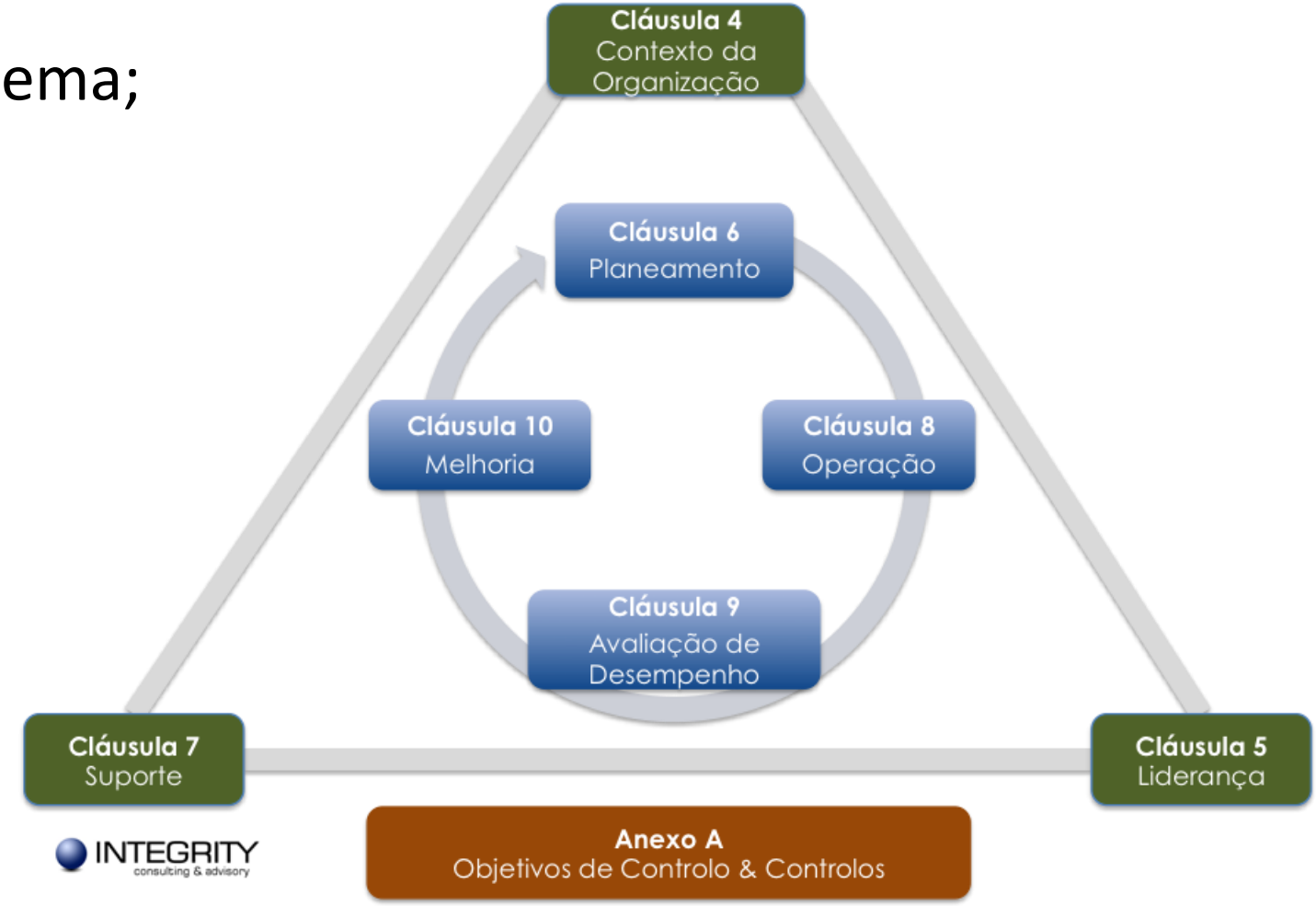
Certificação



Fonte: https://www.27001.pt/iso27001_3.html

Norma 27001

- Esquema;



Fonte: https://www.27001.pt/iso27001_3.html

SGSI

Sistema de Gestão da Segurança da Informação

- Como preparar minha empresa frente ao crime cibernético?
- Programa estruturado para implantação de políticas, normas, diretrizes, procedimentos e orientações para a proteção do conhecimento e da marca da sua empresa;

SGSI

Sistema de Gestão da Segurança da Informação

- Planejamento dos riscos de segurança;
- Implementação de controles detalhados;
- Apoio da empresa;
- 3 pontos essenciais:
  - Avaliar os riscos para a empresa;
  - Avaliar a legislação vigente, os estatutos, a regulamentação e os contratos vigentes e seus parceiros comerciais;
  - A terceira parte são os conjuntos particulares de princípios, objetivos e os requisitos do negócio.

SGSI

Sistema de Gestão da Segurança da Informação

- Porque precisamos?
  - Ataques cibernéticos crescem a cada dia mais;
  - Confiança para os clientes;
  - Diminuição dos riscos;
  - Menos exposição;
  - Garantir a continuidade do negócio.

SGSI

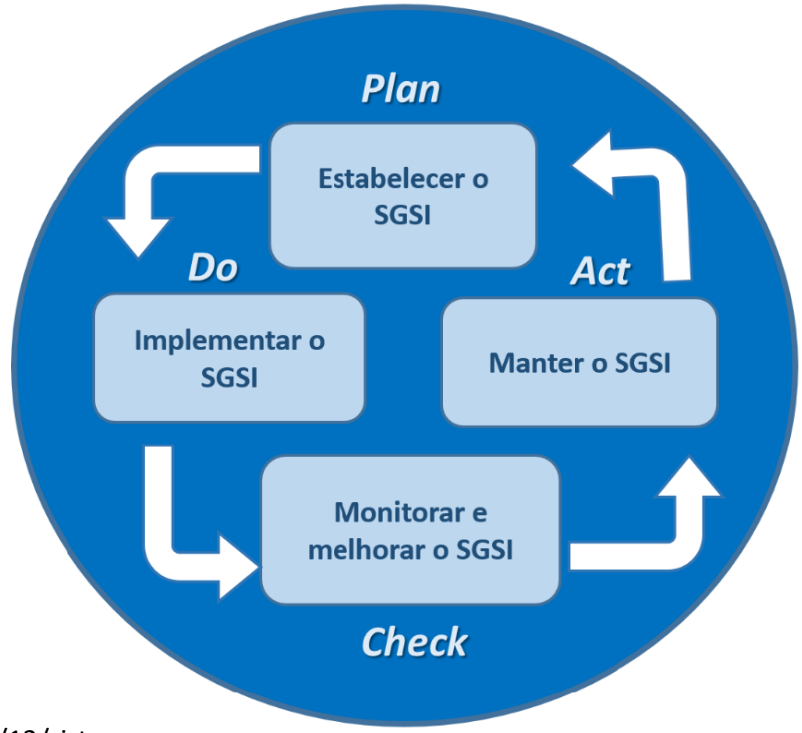
Sistema de Gestão da Segurança da Informação

- Política de Segurança da Informação;
  - Mesa limpa e tela limpa;
  - Backup;
  - Transferência de arquivos;
  - Dispositivos móveis;
  - Controle de acesso lógico e físico;
  - Ativos e comunicações.

SGSI

Sistema de Gestão da Segurança da Informação

- A norma ISO 27001 adota o modelo PDCA (Plan-Do-Check-Act) para descrever a estrutura de um SGSI;



Fonte: https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html

SGSI

Sistema de Gestão da Segurança da Informação

- Estabelecer o SGSI:
  - Criação do SGSI;
  - Suas atividades devem estabelecer políticas, objetivos, processos e procedimentos para a gestão de segurança da informação;
  - Norma 27001: escopo; política; gestão; objetivos e seleção de controles; aplicabilidade.

SGSI

Sistema de Gestão da Segurança da Informação

- Implementar o SGSI:
  - Plano de tratamento de riscos;
  - Implementação do plano;
  - Implementação dos controles;
  - Definir como medir a eficácia dos controles;
  - Gerenciar as operações;
  - Gerenciar os recursos;
  - Implementar os procedimentos.

SGSI

Sistema de Gestão da Segurança da Informação

- Monitorar e analisar criticamente o SGSI:
  - Execução dos procedimentos;
  - Análise crítica regulares da eficácia do SGSI;
  - Eficácia dos controles;
  - Analisar criticamente as avaliações;
  - Auditorias internas do SGSI;
  - Envolver direção na troca de ideias;
  - Atualizar os planos de segurança;
  - Registrar as ações e eventos.

SGSI

Sistema de Gestão da Segurança da Informação

- Boas práticas:
  - Apoio e patrocínio da direção;
  - Tomada de decisão com grupo interdisciplinar;
  - GAP Analysis;
  - Análise de Impacto Empresarial;
  - Estimar os recursos financeiros e ações;
  - Revisão dos padrões de segurança.

Norma 27002

- Boas práticas para Segurança da Informação;
- 27001 define os requisitos e formaliza todo o processo de gestão do SGSI;
- 27002 tem um maior nível de detalhamento e está relacionada ao Anexo A da 27001;
- Implementação de controles é o foco;
- Complementa a 17799.

Norma 27002

- Estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização;
- Melhor conscientização;
- Maior controle dos ativos e informações sensíveis;
- Melhor organização dos processos;
- Conformidade com a legislação;
- Itens de acordo com o Anexo A da 27001 e 17799 – 11 seções.

Norma 27002

- Estrutura

Fonte: https://image.slidesharecdn.com/resumoiso27002-140219200042-phpapp02/95/resumo-iso-27002-2-638.jpg?cb=1392840160

Norma 27003

- Diretrizes para implantação de SGSI;
- Foco na elaboração, planejamento e definição do projeto;
- Ela descreve o processo de obter a aprovação da direção para implementar o SGSI, define um projeto para implementar um SGSI (referenciado nesta Norma como o projeto SGSI), e fornece diretrizes sobre como planejar o projeto do SGSI, resultando em um plano final para implantação do projeto do SGSI.

Norma 27004

- Métricas para o SGSI;
- Avalia a eficácia do projeto;
- Identifica as melhorias a serem implementadas;
- Estrutura dividida em:
  - Racionalidade;
  - Características;
  - Tipos de métricas;
  - Processos.

Norma 27004

Racionalidade

- A necessidade para avaliação;
- Atender aos requisitos da 27001;
- Validar os resultados;
- Benefícios.

Norma 27004

Características

- Monitorar e avaliar as características é o primeiro passo na avaliação do SGSI;
- O que monitorar?
- O que avaliar?
- Quando realizar isto e quais pessoas envolvidas?

Norma 27004

Tipos de Métricas

- Análise de performance – expressam o resultado planejado e o que já foi implementado;
- Análise da eficácia – analisa os efeitos das atividades planejadas e executadas;

Norma 27004

Processos

- As etapas anteriores consistem dos seguintes processos:
  - Identificar as necessidades da informação;
  - Criar e manter medidas de avaliação;
  - Estabelecer procedimentos;
  - Monitorar e medir;
  - Analisar resultados;
  - Avaliar a eficácia dos dados analisados.

Norma 27006

- Auditoria e certificação dos processos formais adotados para o SGSI;
- Trabalha de forma complementar com a 17021-1 e 19011;
- O processo de certificação envolve a auditoria do sistema de gerenciamento de segurança da empresa;
- Dividida em:
  - Requisitos gerais;
  - Requisitos de recursos;
  - Requisitos de informações;
  - Requisitos de processos;
  - Gerenciamento do sistema para certificação.

Norma 27014

- Técnicas de governança de TI;
- A governança da segurança da informação é um sistema pelo qual as atividades de segurança de uma organização são direcionadas e controladas;
- Alinhamento das estratégias e objetivos de negócio com as regras de segurança da empresa.

Norma 27014

- O padrão fornece orientação sobre conceitos e princípios para a governança de segurança da informação, através da qual as organizações podem avaliar, direcionar, monitorar, comunicar e assegurar as atividades relacionadas à segurança da informação dentro da organização e é aplicável a todos os tipos e tamanhos de organizações;
- Devem garantir que as informações sejam compreensíveis e integradas com a empresa.

Norma 27014

- A norma define 6 princípios de alto nível de ações orientadas:
  - Estabelecer a segurança de informação em toda a organização;
  - Adotar uma abordagem baseada em risco;
  - Definir a direção das decisões de investimento;
  - Garantir a conformidade com os requisitos internos e externos;
  - Promover um ambiente positivo para a segurança;
  - Rever o desempenho em relação aos resultados comerciais.

Norma 27031

- Guia para boas práticas de segurança em TIC;
- Abrange todos os eventos e acidentes que podem ocorrer em um sistema;
- Gerenciamento dos incidentes;
- Em certo sentido, falta um pouco de claridade à real proposta desta norma.

Norma 27040

- Norma relacionada à parte de sistemas e infraestruturas;
- Orientações de segurança para o armazenamento dos dados, além da proteção dos mesmos;
- Relacionada à norma 27001;
- Relevante para gerentes e funcionários envolvidos com gerenciamento de risco de segurança da informação dentro de uma organização e, quando apropriado, partes externas que apoiem essas atividades.

Norma 27040

- Em sua estrutura é abordado:
  - Visão geral dos principais conceitos de segurança de armazenamento;
  - Controles que suportam arquiteturas de armazenamento de dados;
  - Diretrizes para a concepção e implementação de segurança de armazenamento (confiabilidade, disponibilidade e resiliência de dados);
  - Termos relacionados à virtualização e computação em nuvem.

Políticas de Segurança

- Documento que deve conter um conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os funcionários, bem como analisado e revisado criticamente, em intervalos regulares ou quando mudanças se forem necessárias;
- ISO/IEC 27001.

Políticas de Segurança

- Basicamente é um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados e é o pilar da eficácia da Segurança da Informação;
- Estabelece regras e normas com o objetivo de diminuir a probabilidade de incidentes;
- Construídas a partir da necessidade do negócio.

Políticas de Segurança

- Adotado por muitas empresas;
- Reconhecimento da necessidade;
- Deve estabelecer como o acesso à informação será feito e de todas as formas possíveis;
- Quais mecanismos a serem usados neste processo.

Políticas de Segurança

Diagnóstico da Segurança da Informação

- Conhecer os ativos da empresa;
- Hierarquizar os ativos da corporação para priorizá-los nas Políticas de Segurança da Informação;
- Avaliar o impacto de cada um no negócio;
- Avaliar ameaças e vulnerabilidades;
- Averiguar se já existe alguma política de segurança na empresa ou ações de prevenção.

Políticas de Segurança

Elaboração da Política de Segurança

- Formar um comitê de segurança da informação;
- Divulgar e estabelecer os procedimentos de segurança;
- Definição de um gestor que tenha responsabilidade na gestão para aprovação do desenvolvimento e avaliação da política de segurança;
- Processos são definidos, como backup, uso de senha, espaços físicos, graus de acesso, planos de contingência e atualização de software.

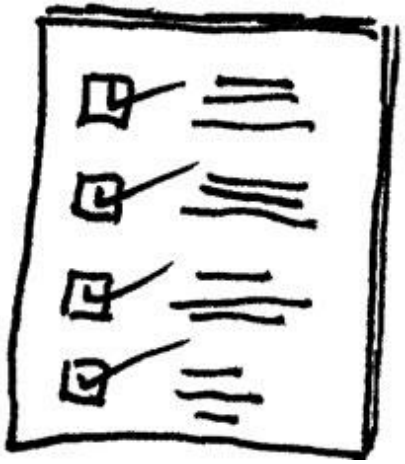
Políticas de Segurança

Implementando da Política de Segurança

- Avisos prévios aos funcionários;
- Política deve ser escrita de forma clara;
- Treinamentos deverão ser aplicados;
- Deixar ciente das ameaças e vulnerabilidades da empresa;
- Contar com o comprometimento da Direção.

Resumo da Aula

- Revisão da Última Aula;
- Norma 27001;
- Norma 27002;
- Norma 27003;
- Norma 27004;
- Norma 27006;
- Norma 27014;
- Norma 27031;
- Norma 27040;
- Políticas de Segurança.



Referências Bibliográficas

- Website – TNEG – https://www.tneg.com.br;
- Website – ISO 27001 – https://www.27001.pt/iso27001_3.html;
- ISO/IEC 27000 ABNT;
- Politica de Segurança da Informação: Definição, Importância, Elaboração e Implementação – Paulo Cesar Oliveira;

Próxima aula

- Prática em laboratório;
  - Cyber Ciege;
- Gestão de segurança;
- Análise diversas normas complementares;
- Análise de Riscos e Ativos.