Arquitetura e Organização de Sistemas Computadorizados - Segurança da Informação

Osmar de Oliveira Braz Junior

Márcia Cargnin Martins Giraldi

Objetivos

- Apresentar a segurança da informação através da norma ISO 27000

Definições

- **1 - Segurança da Informação** – uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.
  - **A segurança como "meio"** – a segurança da informação visa garantir a confidencialidade, integridade e disponibilidade da informação, não repúdio e autenticidade.
  - **A segurança como "fim"** - a segurança da informação é alcançada por meio de práticas e políticas voltadas a uma adequada padronização operacional e gerencial dos ativos, e processos que manipulam e executem a informação.

Definições

- **2 - Informação** – conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processo comunicativos (troca de mensagens) ou transacionais (ex: transferência de valores monetários).
  - legalidade – característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais ou legislação vigente.
- **3 – Ativo** – todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

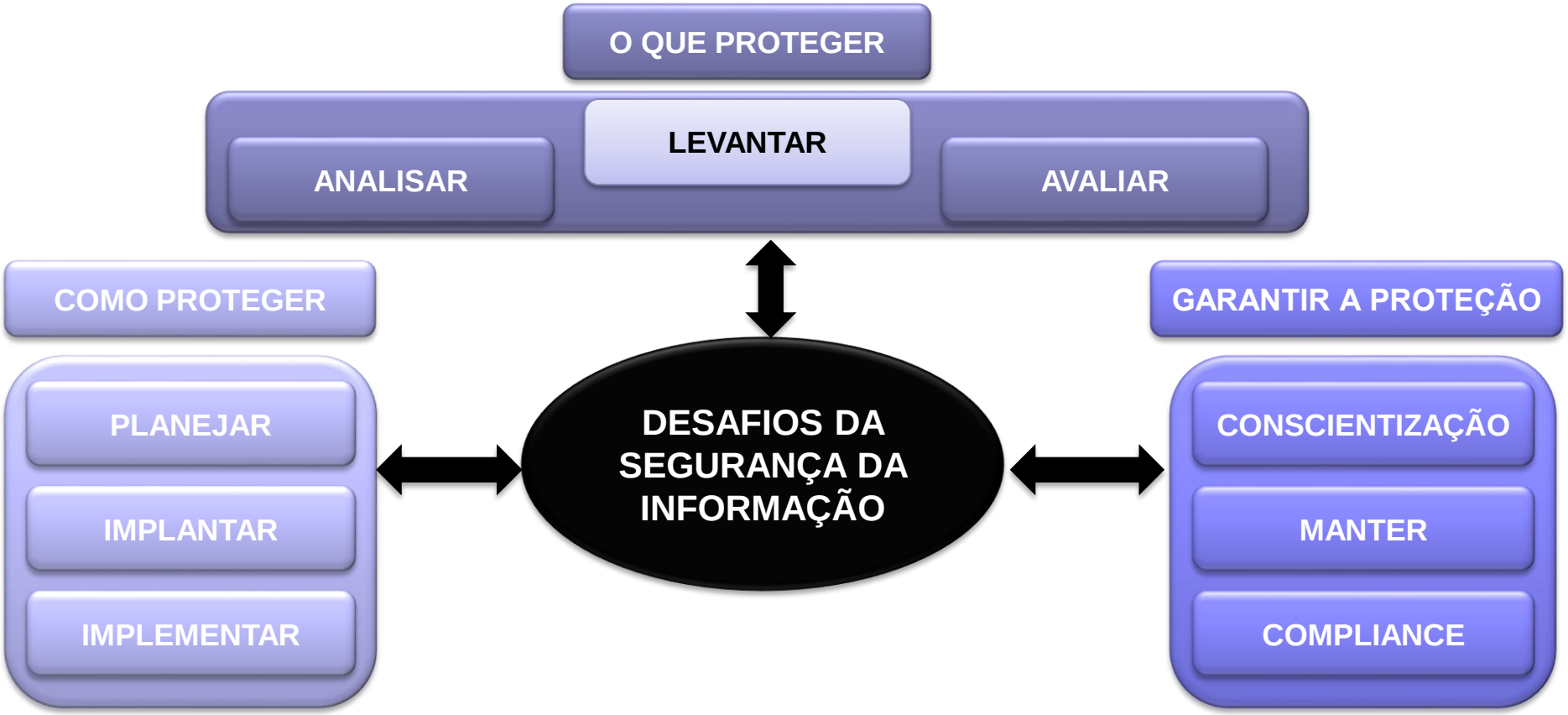
Incidente

- Evento (fato) decorrente da **ação de uma ameaça que explora uma ou mais vulnerabilidades**, levando a perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade.
- Um incidente **gera impactos aos processos de negócio** da empresa, sendo ele o elemento a ser evitado em uma cadeia de gestão de processos e pessoas.

Incidente

- Toda a empresa sofre **ameaças** que tentam **explorar as vulnerabilidades** a fim de acessar as **informações** manipuladas pelos **ativos** que dão suporte a execução dos **serviços** necessários aos **processos de negócio** da empresa.

Desafios da Segurança da Informação



Como implantar

- Como é implantar uma solução de segurança da informação?
- Quais são as fases deste processo?

ISO 27000

- ISO 27000 - Normas que abordam a Segurança da Informação

ISO 27000

- ISO 27001: Gerenciamento da Segurança da Informação
- ISO 27033-3: Segurança em redes de computadores
- ISO 27033-4: Comunicação segura entre rede e Gateways
- ISO 27033-5: Comunicação segura para redes virtuais privadas (VPN)
- ISO 27033-6: Segurança em redes sem fio
- ISO 27036: Segurança da Informação no relacionamento com fornecedores
- ISO 27039: IDS (*Intrusion Detection System*) IPS (*Intrusion Prevention System*)
- ISO 27040: Segurança de Armazenamento

ISO 27000

- Entre as várias ISOs existentes, é a família da ISO 27000 que aborda as normas para a Segurança da Informação.
- Estas normas convertem para o Sistema de Gestão da Segurança da Informação (SGSI), que criam parâmetros para a segurança dos dados digitais e armazenamento eletrônico.
- O SGSI têm os seguintes pilares:
  - Disponibilidade
  - Integridade
  - Confidencialidade

ISO 27000 - Confidencialidade

- A confidencialidade é um pilares mais lembrados quando se fala em segurança
- É a confidencialidade que permite que somente pessoas autorizadas tenha acesso ao necessário
- É ela que por exemplo não autoriza que o colaborador da recepção tenha acesso às notas fiscais emitidas pela empresa

ISO 27000 - Integridade

- Preza para que os dados armazenados e sistemas que a empresa utiliza fiquem mais resistentes à falhas
- A integridade pode ser obtida com as cópias de segurança, tecnicamente chamado de backup. O backup é citado na ISO 27040.

ISO 27000 - Disponibilidade

- Não adianta possuir uma estrutura com boas políticas de confidencialidade e integridade se o sistema não funciona quando os colaboradores precisam utilizar
- Deve ser utilizado por exemplos servidores redundantes, isto é, um segundo servidor que assuma a operação quando o primeiro falhe. Além do clássico nobreak, que permite que servidores e computadores funcionem mesmo quando acontece queda de energia elétrica.

ISO 27000 - Vantagens

- Uma empresa que se torna apta à ISO 27000, cria o reconhecimento da organização com padronização internacional, gera mais credibilidade a seus: clientes, colaboradores e fornecedores

- Para as empresas que já seguem algumas normas, como a ISO 9000, se torna mais fácil a obtenção da ISO 27000, pois a empresa já possui um melhor controle e qualidade em seus procedimentos

ISO 27000 - Vantagens

- Aplicar uma boa gestão é necessário definir os requisitos e metodologias para uma boa gestão
- um dos pontos mais importantes, o levantamento de necessidades da empresa, e como atendê-las
- Benefícios alcançados com a ISO 27001:
  - Detectar e corrigir pontos falhos;
  - conscientização sobre a segurança da informação;
  - Aprimoramento da confiança entre parceiros e clientes;
  - A alta direção assume o controle da gestão da segurança da informação;
  - Mecanismos afim de mensurar o sucesso do sistema;
  - entre outros.

ISO 27000 - Vantagens

- Para uma empresa possuir o certificado ISO 27001, ela deve seguir as seguintes etapas:
  - Definir Objetivo
  - Conhecer as referências normativas
  - Ter ciência dos termos e definições
  - Adotar o Sistema de gestão de segurança da informação (SGSI)
  - A alta gestão deve assumir a responsabilidade na adoção do SGSI
  - Passar por auditorias internas do SGSI
  - Analisar criticamente o SGSI
  - Melhoria constante do SGSI

Atividade – 26-04

Pesquise um estudo de caso da aplicação da ISO 27000 e destaque os seguintes pontos:

- contextualize a empresa/ambiente no qual foi implantado a norma;
- o que motivou a implantação da norma;
- quais os benefícios obtidos;
- comente sobre algum aspecto que chamou a atenção do grupo.

- Links uteis:

  https://ostec.blog/padronizacao-seguranca/primeiros-passos-iso-27000/

  https://www.bsigroup.com/pt-BR/ISO-IEC-27001-Seguranca-da-Informacao/Estudos-de-caso-da-ISOIEC-27001/

  https://scholar.google.com.br/scholar?q=estudo+de+caso+aplica%C3%A7%C3%A3o+iso+27000&hl=pt-BR&as_sdt=0&as_vis=1&oi=scholart

Conclusão

- Conhecemos um pouco sobre de segurança da informação através da norma ISO 27000
- A família de normas é grande, portanto o estudo não termina aqui.

Referências

- WEBER, Raul Fernando. Fundamentos de arquitetura de computadores. 4. ed. Porto Alegre: Bookman, 2012. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788540701434

- STALLINGS, William. Arquitetura e organização de computadores. 8.ed. São Paulo: Pearson, 2010. E-book. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/459/epub/0

- HOGLUND, Greg. Como quebrar códigos: a arte de explorar (e proteger) software. São Paulo: Pearson, 2006. E-book. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/179934/epub/0

Fim