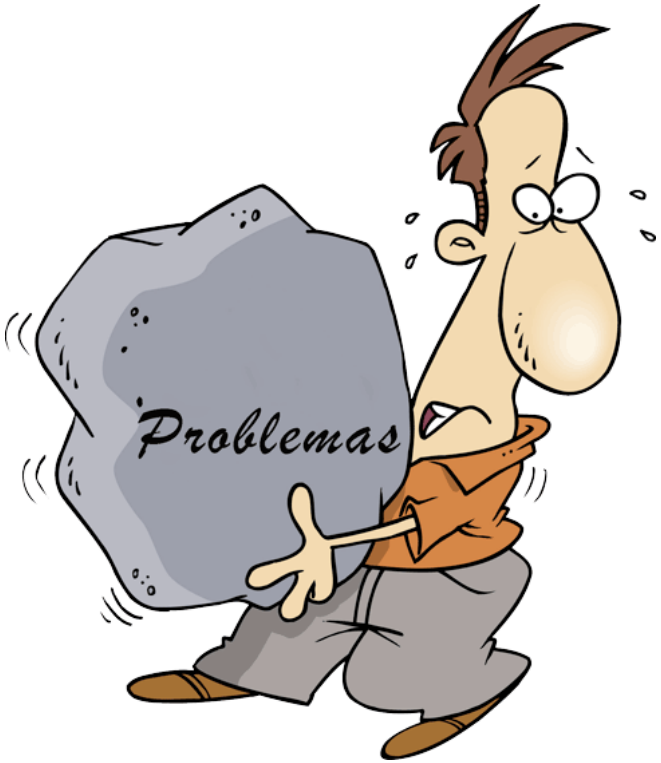
Aula 4 - Planos, procedimentos e políticas de segurança da informação

- Existem diversas dificuldades na implementação da segurança da informação:
  - Os usuários que causam vários problemas e vulnerabilidades no ambiente.
  - Ausência de responsáveis pela SI.
  - Falta de orçamento.
  - Falta de pessoas chave no apoio.
  - Falta de profissionais capacitados.
  - Escopo muito abrangente.
  - Falta de prioridade.
  - Falta de conscientização.



- **ISO 27001** define os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar continuamente Sistema de Gestão de Segurança da Informação (SGSI).

- **ISO 27002** fornece um conjunto detalhado de diretrizes e práticas recomendadas para a implementação eficaz desse sistema.

QUAIS SÃO OS REQUISITOS DA ISO 27001?

01. ANÁLISE DO CONTEXTO DE ORGANIZAÇÃO
Análise e compreensão da empresa e da liderança.

02. AVALIAÇÃO DE RISCO
Elaboração do planejamento e avaliação do suporte.

03. CONTROLES OPERACIONAIS
Implementação dos controles operacionais e tratamento de risco.

04. ANÁLISE DA EFICÁCIA
Monitoramento e análise de desempenho.

05. MELHORIAS
Implementação das ações corretivas.

Norma ISO 27002

- 5.Política de segurança da informação

- 6.Organizando a segurança da informação

- 7.Gestão de Ativos

- 8.Segurança em recursos humanos

- 9.Segurança Física e do Ambiente

- 10.Gerenciamento de operações e comunicações

- 11.Controle de Acesso

- 12.Aquisição, desenvolvimento e manutenção de sistemas da informação

- 13.Gestão de Incidentes de Segurança da informação

- 14. Gestão de Continuidade dos Negócios

- 15.Conformidade

- É importante que as empresas priorizem a segurança de suas informações.

- As empresas devem estabelecer diretrizes e medidas a fim de garantir que todas as atividades sejam conduzidas de acordo com as melhores práticas de segurança da informação.

- É necessário estabelecer padrões para orientar o desenvolvimento de atividades relacionadas à segurança da informação de forma eficaz e consistente.

Política de Segurança da Informação

Intenções e orientações da organização, devidamente formalizadas por sua alta administração

Políticas específicas por tema

Intenções e orientações relacionadas a um assunto específico, definidas pelo nível adequado de gestão

Controle de Acesso	Segurança Física	Gestão de Ativos	Transferência de Informações	Segurança de Redes	Gestão de incidentes de SI	Backup	Criptografia	Classificação de informações	Gestão de vulnerabilidades	Desenvolvimento Seguro

Política de Segurança da Informação

- Uma política nada mais é do que a ação de colocar uma atividade que esteja desorganizada em ordem com base em um conjunto de normas.

- Quando se trata da segurança da informação isso não é diferente. A PSI nada mais é que um conjunto de regras, normas e procedimentos usados para manter a segurança da informação.

- Seu objetivo é orientar as atitudes dos usuários de forma que eles usem os recursos de TI e a informação da maneira mais segura possível.

Política de Segurança da Informação

- Geralmente, a PSI é baseada nas definições da norma ABNT NBR ISO/IEC 27002 (código de boas práticas para a gestão da segurança da informação).

- A PSI define os direitos e principalmente os deveres dos funcionários no uso dos recursos de TI e deve ser apresentada aos funcionários juntamente com um termo de ciência, que deve ser assinado por todos sem distinção.

- A PSI deve ser uma medida PREVENTIVA, mas a maioria das empresas a usa de maneira CORRETIVA, criando a mesma apenas depois que problemas já ocorreram.

- Sua elaboração deve envolver pessoas das diversas áreas da empresa para envolver todos os aspectos possíveis do negócio.

  - **Comitê Gestor de Segurança da Informação**
    - O Comitê Gestor de Segurança da Informação tem como competência atuar no planejamento, coordenação, supervisão, execução e controle de políticas e normas relativas à Segurança da Informação.

- Cada empresa deve ter sua política de segurança, de acordo com seu cenário organizacional, com seus ativos e com as ameaças que podem atingir seu negócio. Não existe uma receita pronta!!!

- Uma PSI é composta por várias normas, cada uma tratando de um assunto específico.

A Política de Segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação

Vantagens

- Padronização
- Alinhamento a leis externas
- Definição de responsabilidades
- Definição de penalidades
- Conscientização dos colaboradores

- A PSI deve:
  - Ser formal dentro da empresa
  - Ser clara e objetiva
  - Ser plausível
  - Usar linguagem simples
  - Ser de fácil compreensão e aplicabilidade
  - Deve ser aplicada a todos
  - Ser revisada e atualizada periodicamente
  - Ter punições claras

Etapas da Elaboração da PSI

1. **Definir os objetivos e escopo:** Determine os objetivos específicos da política de segurança da informação e o escopo dela. Isso pode envolver a proteção de dados confidenciais, sistemas de TI, dispositivos móveis, acesso físico a instalações, etc.

2. **Analisar o ambiente:** Realize uma análise detalhada do ambiente da organização, identificando os ativos de informação, ameaças potenciais e vulnerabilidades presentes nos sistemas, processos e pessoas.

3. **Identificar requisitos legais e regulatórios:** Identificar quais leis e regulamentos são relevantes para a área e a região em que a organização opera. Garantir de que a política esteja em conformidade com esses requisitos.

4. **Definir responsabilidades:** Atribuir responsabilidades claras para a implementação e manutenção da política de segurança da informação. Isso pode incluir papéis como o CISO (Chief Information Security Officer), gerentes de TI, administradores de sistemas, funcionários de segurança, etc.

5. **Desenvolver diretrizes de segurança:** Criar diretrizes claras e específicas para a segurança da informação. Isso pode abranger áreas como autenticação, controle de acesso, criptografia, proteção de dispositivos móveis, políticas de senhas, etc.

6. **Estabelecer controles de segurança:** Definir os controles técnicos e organizacionais que serão implementados para mitigar riscos. Isso pode incluir firewalls, sistemas de detecção de intrusões, políticas de uso aceitável, treinamento de conscientização em segurança, etc.

7. **Criar diretrizes de gestão de incidentes**: Desenvolver um plano para lidar com incidentes de segurança da informação, incluindo procedimentos para relatar, investigar e responder a violações de segurança.

8. **Comunicar a política:** Garantir que a política de segurança da informação seja clara e compreensível para todos os funcionários. Realize treinamentos e campanhas de conscientização para garantir que todos estejam cientes das diretrizes e responsabilidades.
   - Todos os usuários devem, **OBRIGATORIAMENTE**, assinar um termo de ciência da PSI.

9. **Revisar e aprovar:** Submeter a política de segurança da informação para revisão e aprovação pelas partes relevantes na organização, como a alta administração e a equipe jurídica.

10. **Implementar e monitorar:** Colocar a política em prática e monitorar sua implementação. Isso pode envolver a configuração de sistemas de monitoramento, auditorias regulares e avaliações de conformidade.

11. **Revisar e atualizar:** A política de segurança da informação deve ser revisada periodicamente para garantir que ela permaneça eficaz diante das mudanças no ambiente de segurança, tecnologia e regulamentações.

12. **Lidar com mudanças:** Adaptar a política sempre que ocorrerem mudanças significativas na organização, como a introdução de novas tecnologias, expansão para novos mercados ou alterações regulatórias.

Camadas de Aplicação da PSI

- **Estratégica:** define o rumo a ser seguido (política geral da segurança da informação);
- **Tática:** define a padronização para melhor controlar (políticas ou normas complementares) e fazer com que todos os pontos da empresa tenham o mesmo nível de segurança;
- **Operacional:** define os procedimentos e orientações (“step by step”) dos processos.


POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO
Políticas
ESTRATÉGICO
POLÍTICAS COMPLEMENTARES (NORMAS)
Normas e Padrões
TÁTICO
PROCEDIMENTOS OPERACIONAIS PADRÃO (POPs)
Procedimentos e Orientações
OPERACIONAL

- Itens que devem existir em cada norma da PSI:
  1. Descrição
  2. Objetivo
  3. Deveres do usuário
  4. Deveres do administrador
  5. Recomendações
  6. Penalidades

- Exemplo:
  1. **Descrição: Norma 1 – uso do correio eletrônico corporativo**
  2. **Objetivo:** garantir a correta utilização do email, evitando problemas legais para a empresa
  3. **Deveres do usuário:** não propagar spams, correntes, conteúdo pornográfico, político ou religioso
  4. **Deveres do administrador:** garantir a disponibilidade do serviço
  5. **Recomendaçõe**s: não divulgar o email em fóruns da internet
  6. **Penalidades :** o não cumprimento do item 3 dessa norma acarretará em advertência na primeira ocorrência, suspensão não remunerada de 2 dias na segunda ocorrência e demissão na terceira ocorrência

- Algumas normas que podemos ter na PSI:
  - Norma de Backups;
  - Norma de segurança Física;
  - Norma de segurança Lógica;
  - Norma de controles de acessos;
  - Norma do uso da internet;
  - Norma do uso do correio eletrônico;
  - Norma de utilização de computadores e notebooks dentro ou fora da organização;
  - Norma do uso do ambiente sem fio;
  - Norma de instalação e utilização de programas...

Atividade (em grupo) – Normas da PSI

- Conforme explicado cada grupo deverá criar uma norma que pode fazer parte da PSI de uma empresa. Usar o exemplo da aula como modelo, pode também ser escolhido uma das normas apresentadas para a elaboração.

Os 4 P’s da PSI

- Existem diversas filosofias de implantação da PSI em uma empresa.

Paranoico: tudo é proibido, mesmo o que deveria ser permitido

Proibitivo: tudo que não é permitido é explicitamente proibido

Permissivo: tudo que não é proibido é explicitamente permitido

Promíscuo: tudo é permitido, mesmo o que deveria ser proibido

- Exemplo: Acesso à Internet
  - Paranóico: sem acesso
  - Proibitivo: controle através de lista de sites bloqueados
  - Permissivo: controle através de lista sites permitidos
  - Promíscuo: sem controle

Vídeos

- 4 – política de segurança da informação 1 - https://www.youtube.com/watch?v=AIZOcikPX8w&index=4&list=PLKh209jb160eYwx5FZ4zlfsKwi-bYOqkQ&t=37s
- 4 – política de segurança da informação 2 - https://www.youtube.com/watch?v=sI53y8Nnuf0&list=PLKh209jb160eYwx5FZ4zlfsKwi-bYOqkQ&index=2

Exercícios de Fixação

1. Dentre as opções abaixo, qual deles NÃO é um desafio para a implantação da política de segurança?

A. Falta de profissionais capacitados
B. Escopo muito abrangente
C. Falta de conscientização dos funcionários
D. Orçamento liberado

1. Dentre as opções abaixo, qual deles NÃO é um desafio para a implantação da política de segurança?

A. Falta de profissionais capacitados
B. Escopo muito abrangente
C. Falta de conscientização dos funcionários
D. Orçamento liberado

2. Como podemos definir a PSI (Política de Segurança da Informação)?

A. Norma definida pela ISO para boas práticas em SI
B. Conjunto de leis, normas, regras e procedimentos para a manutenção da SI na empresa
C. Conjunto de regras que trata exclusivamente do controle de acesso físico do data center
D. Lei americana voltada para o mercado financeiro

2. Como podemos definir a PSI (Política de Segurança da Informação)?

A. Norma definida pela ISO para boas práticas em SI

B. Conjunto de leis, normas, regras e procedimentos para a manutenção da SI na empresa

C. Conjunto de regras que trata exclusivamente do controle de acesso físico do data center

D. Lei americana voltada para o mercado financeiro

3. Sobre a PSI, é correto afirmar que:

A. É fácil de implantar em qualquer empresa
B. Não depende em absolutamente nada dos usuários
C. Deve ser elaborada e colocada em prática antes de os problemas ocorrerem
D. Uma PSI pode ser usada em qualquer empresa, não havendo necessidade nenhuma de criar algo de acordo com o cenário da empresa

3. Sobre a PSI, é correto afirmar que:

A. É fácil de implantar em qualquer empresa
B. Não depende em absolutamente nada dos usuários
C. Deve ser elaborada e colocada em prática antes de os problemas ocorrerem
D. Uma PSI pode ser usada em qualquer empresa, não havendo necessidade nenhuma de criar algo de acordo com o cenário da empresa

4. Qual camada da organização irá discutir e tomar decisões sobre diretrizes estratégicas e de negócio?

A. Estratégica
B. Tática
C. Operacional
D. Braçal

4. Qual camada da organização irá discutir e tomar decisões sobre diretrizes estratégicas e de negócio?

A. **Estratégica**
B. Tática
C. Operacional
D. Braçal

Atividade (em grupo)

- Estudo de caso para análise de vulnerabilidades e propostas de medidas de segurança