

# SEGURANÇA E PROTEÇÃO DE DADOS

Prof. Priscilla Cunha

[pcunha@uni9.pro.br](mailto:pcunha@uni9.pro.br)

# Agenda

 <b>DIFICULDADES NA SEGURANÇA DA INFORMAÇÃO</b>	 <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI</b>	 <b>VANTAGENS DA PSI</b>
 <b>ETAPAS DA ELABORAÇÃO DA PSI</b>	 <b>OS 4 P'S DA PSI</b>	 <b>VÍDEOS</b>
 <b>PARA SABER MAIS</b>	 <b>Dicas para Estudo</b> <ul style="list-style-type: none"><li> <b>Seja "CURIOSO":</b> Experimente a prática, pesquise, registre e informe a sua equipe.</li><li> <b>Seja "ATENADO":</b> Não se distraia.</li><li> <b>Seja "COLABORATIVO":</b> Seja sempre colaborativo para ajudar a equipe.</li><li> <b>Prof. Priscila Cunha</b></li></ul>	



# DIFICULDADES NA SEGURANÇA DA INFORMAÇÃO

- Quando se trata de segurança da informação, diversas dificuldades são encontradas no processo de sua implementação. Algumas dessas dificuldades já estamos discutindo a algumas semanas, como é o caso dos usuários que causam vários problemas e vulnerabilidades no ambiente.
- Mas temos outras dificuldades, como veremos a seguir, e que causam muitos problemas.



Ausência de responsáveis pela SI: muitas empresas não possuem um departamento de segurança para implementar os procedimentos adequados.



Falta de orçamento: apesar de segurança envolver muitos procedimentos e regras, é preciso também investir em hardware, software e certificações.

Falta de pessoas chave no apoio: o apoio e aval da alta administração da empresa é primordial para que as pessoas na empresa se comprometam com a implementação das medidas adotadas.

Falta de profissionais capacitados: é de extrema importância que o pessoal de SI seja capacitado na área, e não pessoas aproveitadas de outras áreas.

- Escopo muito abrangente: às vezes a necessidade de segurança em uma empresa é tão amplo, que o projeto de implementação da segurança se torna algo “monstruoso” e impossível de se colocar em prática. Quando isso ocorre, se o projeto não for dividido em partes menores a chance de sucesso fica muito reduzida.

- Falta de prioridade: grande parte das empresas se preocupa com a segurança depois de muitas outras coisas, deixando a área sem prioridade.



- Falta de conscientização: olha nós aqui, novamente, falando do usuário e sua falta de consciência com a segurança da informação da empresa.... Esse é, provavelmente, nosso maior problema e que requer medidas intensivas e drásticas, como treinamentos contínuos e penalidades claras.

- Atualmente, é fundamental que as empresas zelem pela segurança de suas informações.
- Para tal, definem diretrizes e meios a fim de que todas as atividades estejam de acordo com as melhores maneiras de serem desenvolvidas, ou seja, as empresas definem padrões de desenvolvimento de atividades relacionadas com a segurança.



# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

- Uma política, qualquer que seja sua área de abrangência, 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.
- Geralmente, a PSI é baseada nas definições da norma ABNT NBR ISO/IEC 27002, (código de prática para a gestão da segurança da informação).

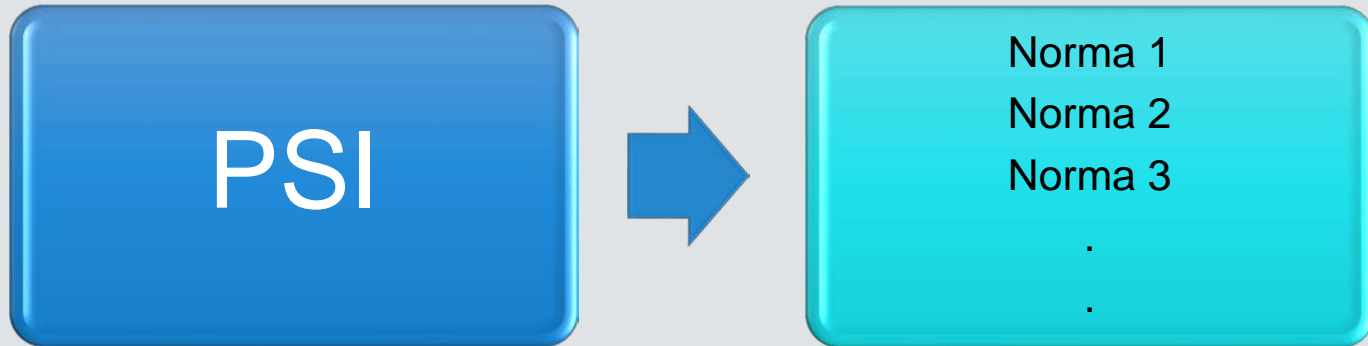
- A PSI define os direitos e principalmente os deveres dos funcionários no uso dos recursos de TI e deve ser apresentada aos funcionários juntamente com um termo de ciência, que deve ser assinado por todos sem distinção.

- 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.



- 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 DA PSI**

Padronização



Alinhamento a leis externas

Definição de responsáveis pelos ativos de TI

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

Ter o apoio e aval da alta administração;

Fazer um levantamento da empresa e sua necessidade de segurança;

Identificar quais são as iniciativas de segurança da empresa e os controles existentes;

Identificar e classificar todas as informações da empresa;



Definir as normas que serão criadas;

Desenvolver o conteúdo da PSI;

Divulgar a PSI;

Treinar e conscientizar os usuários;

Todos os usuários devem, OBRIGATORIAMENTE, assinar um termo de ciência da PSI.

# Camadas de Aplicação da PSI



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



- Itens que devem existir em cada norma da PSI:
  - Descrição
  - Objetivo
  - Deveres do usuário
  - Deveres do administrador
  - Recomendações
  - 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. Recomendações: 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 do uso da computação móvel;
  - 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.



# OS 4 P'S DA PSI

- Existem diversas filosofias de implantação da PSI em uma empresa.
- Podemos citar os principalmente tipos :



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

Proibitivo: tudo que não é permitido é explicitamente proibido

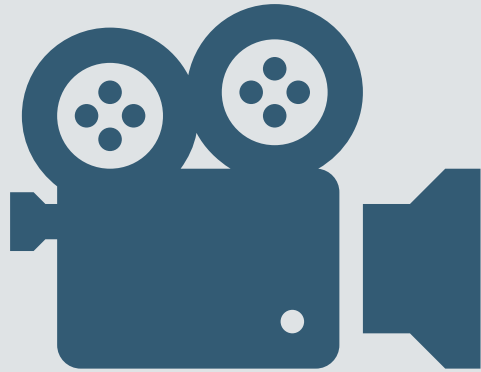
Permissivo: tudo que não é proibido é explicitamente permitido

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**



- Política de segurança da informação - <https://www.youtube.com/watch?v=AIZOcikPX8w&index=4&list=PLKh209jb160eYwx5FZ4zIfsKwi-bYOqkQ>
- Política de segurança da informação - <https://www.youtube.com/watch?v=sI53y8Nnuf0&list=PLKh209jb160eYwx5FZ4zIfsKwi-bYOqkQ&index=2>
- Política de segurança da informação - <https://www.youtube.com/watch?v=nQ2ptWBr-Rw>

