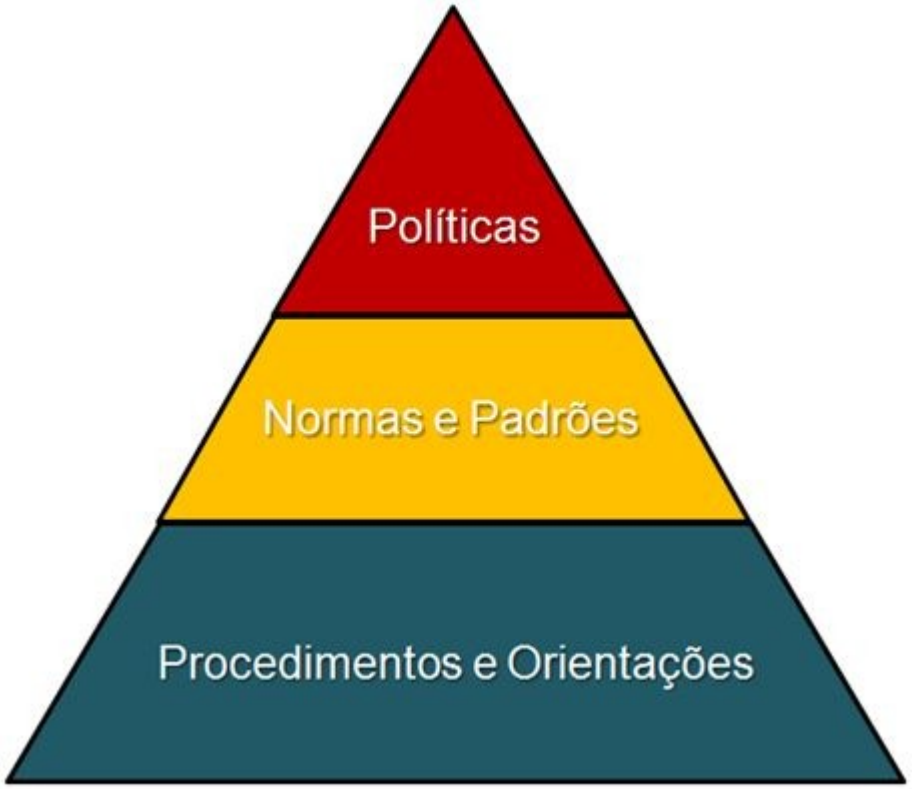
Segurança da Informação e Proteção ao Conhecimento

Aula 07 – Política de Segurança da Informação



Prof. Dalton Martins
dmartins@gmail.com

Gestão da Informação
Faculdade de Informação e Comunicação
Universidade Federal de Goiás

Política de segurança da informação

Definição

- Conjunto de regras gerais que direcionam a segurança da informação e são suportadas por normas e procedimentos.
- Devem ser seguidas por toda a organização, orientando a segurança da informação, conforme o ramo de negócio, legislação e normas vigentes.
- A política de segurança deve ser clara e objetiva.
- E pode ser considerada um documento jurídico.

Diagrama

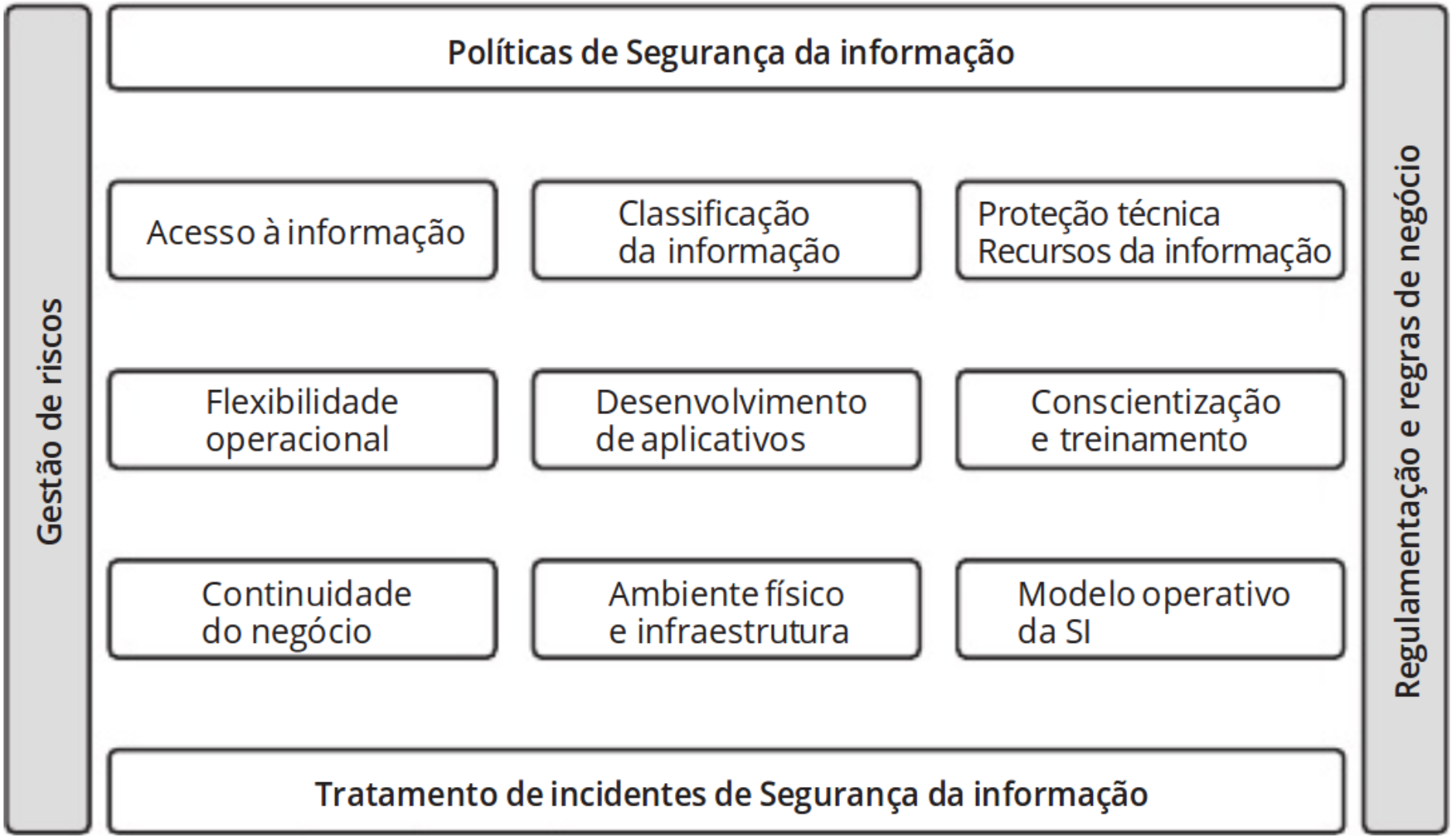
Figura 4.1
Sequência e relação da política de segurança com fases do planejamento.

Políticas	Diretrizes que devem ser seguidas. Responde ao "porquê" de realizar a Segurança da Informação, definindo diretrizes genéricas do que deve ser realizado pela organização para alcançar a Segurança da informação.
Normas	Regras básicas de como deve ser implementado o controle ou conjunto de controles, que foram definidos nas políticas. Respondem "o quê" fazer para se alcançar as diretrizes definidas na política de segurança.
Procedimentos	Atividades detalhadas de como deve ser implementado o controle ou conjunto de controles. Respondem "como" fazer cada item definido nas normas específicas e suas políticas.
Instruções	Descrição de uma operação ou conjunto de operações para a execução da implementação de controles de segurança da informação.
Evidências	Mecanismos adotados para permitir a coleta e comprovação da aplicação dos controles de segurança da informação, sua eficácia e eficiência. Permitirá a rastreabilidade e uso em auditorias.

Tabela 4.1
A Política de segurança da informação em detalhes.

Arquitetura das políticas de segurança

Não existe uma arquitetura padrão para a definição das políticas de segurança. Elas devem seguir e atender aos requisitos de negócios da organização e sua cultura organizacional. Para uma boa estruturação das políticas de segurança, podemos ter por base as dimensões da segurança da informação apresentadas no livro *Praticando a Segurança da Informação*:



Questionamentos importantes

- O que se quer proteger?
- Contra o quê ou quem?
- Quais são as ameaças mais prováveis?
- Qual a relevância de cada recurso?
- Qual o grau de proteção requerido?
- Quanto tempo, recursos financeiros e humanos se pretende gastar?
- Quais as expectativas dos usuários e clientes?

Etapas

- Identificar a legislação.
- Identificar recursos críticos.
- Analisar necessidades de segurança.
- Elaborar proposta e promover discussão aberta.
- Apresentar documento.
- Aprovar e implementar.
- Comunicar e treinar.
- Manter a política de segurança.

Identificar a legislação

Toda organização é submetida a várias leis, regulamentações, normas do órgão regulamentador da sua área de negócios, que devem ser seguidas e atendidas sob o risco grave de penalidades no caso de não cumprimento. Assim, é importantíssimo o levantamento de toda legislação para que as políticas de segurança não venham a atentar contra qualquer uma delas.

Identificação dos recursos críticos

- Hardware.
- Software.
- Dados.
- Pessoas.
- Documentação.
- Suprimentos.
- Entre outros.

Análise das necessidades de segurança

Engloba a análise de riscos:

- Ameaças e impactos.

Busca-se identificar:

- Componentes críticos.
- Grau de proteção adequado.
- Custos potenciais.
- Adequação às boas práticas.

Elaboração da proposta e discussão aberta

A proposta deve contemplar:

- Recursos críticos.
- Análise das necessidades de segurança.

A proposta deve ser discutida entre os envolvidos:

- Dirigentes da organização, em especial.

Documentação

- Definição de segurança da informação, suas metas, escopo e importância.
- Declaração do comprometimento dos dirigentes da organização.
- Objetivos de controle e os devidos controles.
- Análise, avaliação e gerenciamento de riscos.
- Explanação resumida das políticas, princípios, normas e requisitos.
- Definição das responsabilidades gerais e específicas quanto à gestão da segurança.
- Referências a documentos que apoiem a política.

Aprovação e implementação

- Aprovação, em especial dos dirigentes da organização.
- Implementação.

Comunicação da política e treinamento

A divulgação da política de segurança e sua comunicação a toda a organização é outro aspecto importante para sua implementação. Recomenda-se, a propósito, que a divulgação faça parte de programas de formação de funcionários novatos e de reciclagem dos antigos, além de ser efetuada periodicamente. Essa divulgação da política deve ser formal e efetiva, informando todos os detalhes da sua implementação, como deve ser cumprida e as penalidades, se for o caso, da sua não observância. Lembre-se de que a melhor medida de prevenção é a educação.

Manutenção

A política de segurança deve ser analisada periodicamente ou quando ocorrerem mudanças significativas. Deve considerar:

- Oportunidades para melhoria.
- Mudanças no ambiente organizacional (negócios, legislação ou tecnologias).
- Tendências de ameaças e vulnerabilidades.
- Incidentes de segurança ocorridos.

Boas práticas

- Apoio explícito da alta direção.
- Determinar o que fazer para cada tipo de potencial violação à política de segurança.
- Estabelecer uma estrutura organizacional de responsabilidades.
- Estabelecer procedimentos de segurança de pessoal.
- Informar a todos os envolvidos os riscos e suas responsabilidades.

Boas práticas

- Controlar e classificar os recursos computacionais disponíveis.
- Estabelecer controles de acesso lógico e físico.
- Administrar os recursos computacionais segundo os requisitos de segurança.
- Auditar a segurança periodicamente.

Boas práticas para escrever o texto da política

- Definir o objetivo do documento.
- Usar textos curtos e objetivos, escritos na linguagem do público da organização.
- Definir papéis e responsabilidades.
- Evitar o uso de termos técnicos ou em língua estrangeira.
- Evitar o uso de "não".
- Evitar o uso de "exceto" ou "em princípio".
- Criar na política um item para as definições e conceitos.
- Penalização. Utilizar a colaboração do Jurídico e do RH.
- Criar regras e recomendações factíveis de serem aplicadas e cumpridas.
- Atentar para a correção gramatical. Evitar gírias e termos de duplo sentido.
- Solicitar que o Jurídico da organização avalie.

- Definir o objetivo do documento: descrever qual o objetivo do documento e o que a organização deseja comunicar com o documento da política;
- Usar textos curtos e objetivos, escritos na linguagem do público da organização. Seja claro na mensagem que deseja passar, de tal forma que o texto seja entendido por todos. Seja explícito e não deixe dúvidas ou incertezas;
- Definir papéis e responsabilidades com relação à política de segurança;
- Evitar o uso de termos técnicos ou em língua estrangeira. Ninguém é obrigado a conhecer a terminologia técnica que não é da sua área de atuação;
- Evitar o uso de "não". Caso necessário utilizar "é proibido", "negar", "é vedado", entre outras;
- Evitar o uso de "exceto" ou "em princípio". Esses termos deixam a abertura para desculpas por não cumprimento;
- Criar na política um item para as definições e conceitos. Definir no início do documento todos os conceitos, definições, termos técnicos e siglas que serão empregados nas políticas;
- Penalização. Definir as possíveis penalidades para aqueles usuários que não cumprirem a política. Utilizar a colaboração do Jurídico e do RH;
- Criar regras e recomendações factíveis de serem aplicadas e cumpridas por toda a organização e em todos os níveis hierárquicos;
- Atentar para a correção gramatical. As políticas devem ser exemplo da apresentação escrita da linguagem. Evitar gírias e termos de duplo sentido;
- Solicitar que o Jurídico da organização avalie e aponha o seu "de acordo".

Atividade 4.2 – Elaborando uma política de segurança da informação

Você foi designado(a) para apresentar uma proposta de política de segurança para o serviço de correio eletrônico na sua instituição. Descreva e justifique as etapas que adotará para concluir uma proposta:

Quem deverá aprovar sua proposta? Justifique sua resposta.

Atividade 4.3 – Implementando uma política de segurança

Qual a atividade essencial após a conclusão e aprovação da política?

Apresente a sua justificativa.

Atividade 4.4 – Desenvolvendo uma política de segurança na sua organização

Como responsável pela área de TI, você foi designado(a) para compor o Comitê de Segurança da Informação da sua organização. O comitê atualmente está fazendo a revisão de alguns textos de políticas de segurança.

1. Analise os textos da política a seguir, aponte os erros existentes e reescreva-os:

a. Os usuários não devem empregar clientes de Internet Service Provider (ISP) e linhas dial-up para acessar a internet com os computadores da organização X. Toda atividade de acesso à internet deve passar através dos firewalls da organização X, de modo que os controles de acesso e os mecanismos de segurança possam ser aplicados.

b. Um documento que possua informação classificada como secreta ou altamente confidencial nunca pode ser enviada a uma impressora da rede sem que lá esteja uma pessoa autorizada para proteger sua confidencialidade durante e após a impressão.

c. Os geradores secundários e backup de energia devem ser empregados onde seja necessário para assegurar a continuidade dos serviços durante falhas ou falta de energia elétrica.

2. Em uma reunião do comitê, foi perguntado a você, como especialista no assunto, que apresentasse quais devem ser as primeiras políticas de segurança a serem trabalhadas e desenvolvidas. Qual a sua resposta? Justifique.