

Curso de Ciência da Computação**Disciplina: Segurança e Auditoria da Informação - 8º período****Professor: José Maurício S. Pinheiro****AULA 1 – Conceitos e Normas para Segurança da Informação****1. Sistemas, Processos e Informações**

Ao observarmos o funcionamento de um setor específico ou uma organização em sua totalidade, podemos verificar a existência de um padrão na forma como os diversos recursos (equipamentos, procedimentos, informações entre outros) juntamente com as pessoas se configuram, fato este que se repete inclusive em organizações de diversos portes e com características de operação diferentes.

Desta forma se pode perceber que o controle da informação é essencial para o monitoramento eficiente dos procedimentos. Com base nesta linha de argumentos surgem as seguintes questões:

- Seria possível estabelecermos um modelo genérico para estudo e compreensão de uma organização e suas respectivas áreas?
- Como compreender, classificar e modelar os fluxos de informações intra e extra-organizacionais?

1.1. Sistemas

O termo Sistema poderia ser definido como “Conjunto de partes, componentes, que interagem entre si, de forma ordenada, a fim de atingir um objetivo comum. De acordo com esse conceito, todos os sistemas têm partes que interagem entre si, possuem ordem ou normas e visam um objetivo comum.

Outra forma de se analisar um sistema seria através do modelo baseado em entradas, componentes, saídas e *feedback*. Neste modelo as entradas correspondem a tudo aquilo que o sistema necessita para operar e que são recursos obtidos externamente. Componentes correspondem aos procedimentos internos do sistema, necessários para a transformação dos elementos de entrada. Já as saídas correspondem aos resultados que o sistema devolve ao meio externo. *Feedback* corresponde a tipos de saídas que servem de referência para modificar as entradas e/ou processamento, por exemplo, ao se analisar a queda das vendas através de um relatório, os gestores decidem modificar as políticas de preço da empresa (processamento). A Figura 1 se propõe a demonstrar graficamente o relacionamento envolvendo: entradas, componentes, saídas e retroalimentação.

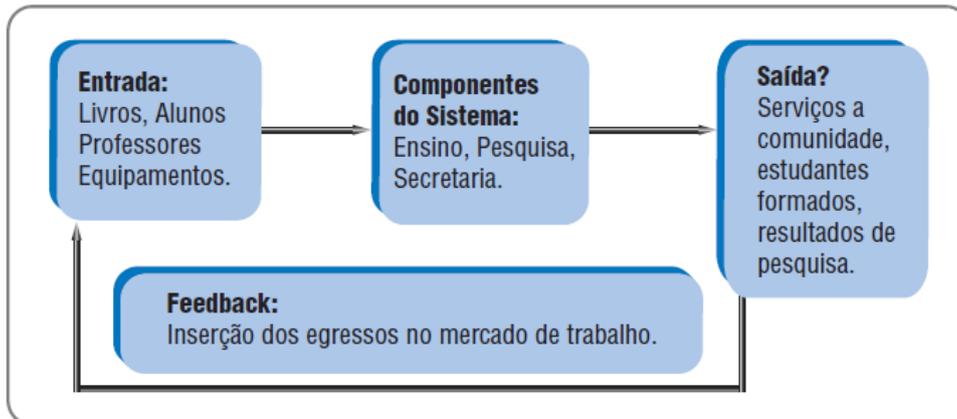


Figura 1 - Mecanismo de funcionamento de um sistema Universidade.

1.1.1. Classificação de Sistemas

Os sistemas podem ser classificados de inúmeras formas, que não são mutuamente excludentes. A seguir, temos as principais:

- **Aberto e Fechado:** Sistemas abertos são aqueles que possuem um elevado grau de interação com o ambiente. As organizações assim como os seres vivos necessitam interagir com o meio externo, realizando trocas de recursos e informações em todos os níveis da organização. Os sistemas fechados são o oposto, contudo vale a ressalva de que não é possível a existência de um sistema completamente fechado, o que ocorre são graus diferentes de interação. Assim um sistema de uma organização militar tende a ser considerado como mais fechado que um sistema de uma instituição bancária.
- **Adaptável e Não-Adaptável:** Os sistemas adaptáveis são aqueles que respondem adaptativamente às mudanças do ambiente através de um monitoramento contínuo. Os Não-Adaptáveis não prevêm mudanças significativas diante das alterações do ambiente. No contexto organizacional, as empresas vistas como sistemas não-adaptáveis normalmente não sobrevivem às turbulências do ambiente de negócio.
- **Sistemas Permanentes e Temporários:** Os permanentes são sistemas sem um prazo predeterminado para deixar de existir. De maneira geral, uma organização não estabelece um horizonte de vida. Os Sistemas temporários têm um tempo de operação pré-definido, por exemplo, um sistema composto por pessoas e recursos para executar um projeto específico.

De acordo com as classificações acima, podemos inferir que um sistema pode ser classificado simultaneamente em diversas categorias: Por exemplo, um consórcio de empresas formado para participar de uma concorrência específica pode ser classificado como: Aberto, adaptável e temporário.

1.2. Sistema de Informação

É um tipo especializado de Sistema, que é formado por um conjunto de componentes, inter-relacionados, que visam coletar dados e informações, manipulá-los e processá-los para finalmente dar saída à novos dados e informações.

Em um Sistema de Informação consideramos que os elementos de entrada e saída são sempre dados e ou informações, e o conjunto dos procedimentos do processamento não envolvem atividades físicas e sim manipulação, transformação de dados em informação conforme pode ser observado na Figura 2, a seguir.

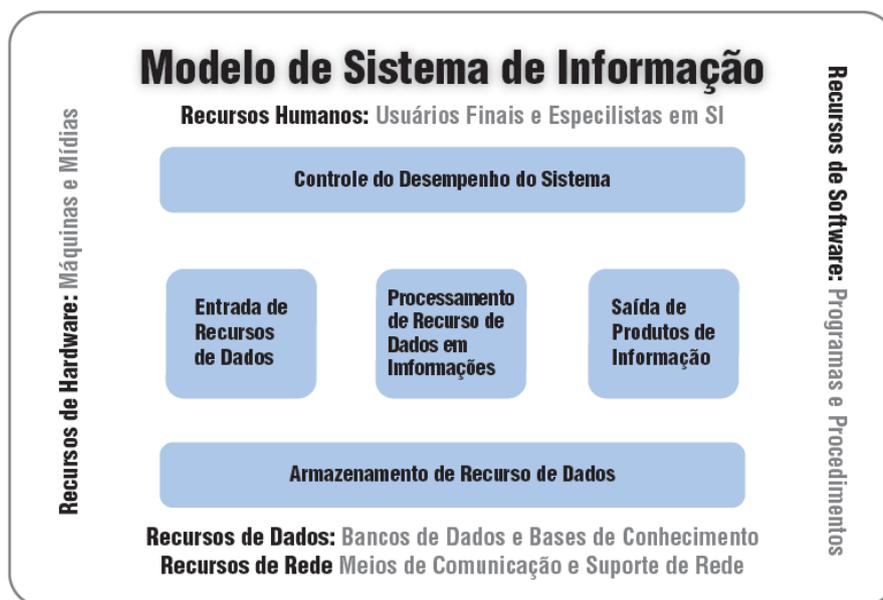


Figura 2 - Modelo de Sistema de Informação

Na figura anterior observam-se os diversos componentes de um Sistema de Informação (Entrada, Processamento e Saída), os mecanismos de armazenamento e controle do sistema, além dos diversos recursos (Hardware, Redes, Software entre outros) que oferecem Suporte.

2. Classificação dos Sistemas de Informação Segundo o Nível Organizacional

Tal classificação apresenta como critério de categorização o nível organizacional aos quais os sistemas de informação buscam atender. Assim são definidas três categorias essenciais:

- Os Sistemas de Processamento de Transação (SPT) que atendem ao nível operacional da organização.
- Os Sistemas de Informações Gerenciais (SIG) que atendem ao nível gerencial.

- Sistemas de Apoio à decisão (SAD) ou Sistemas de Suporte à Decisão (SSD) que visam atender às necessidades do nível estratégico da organização.

A Figura 3, procura relacionar os tipos de sistemas de informação aos respectivos grupos de usuários envolvidos.

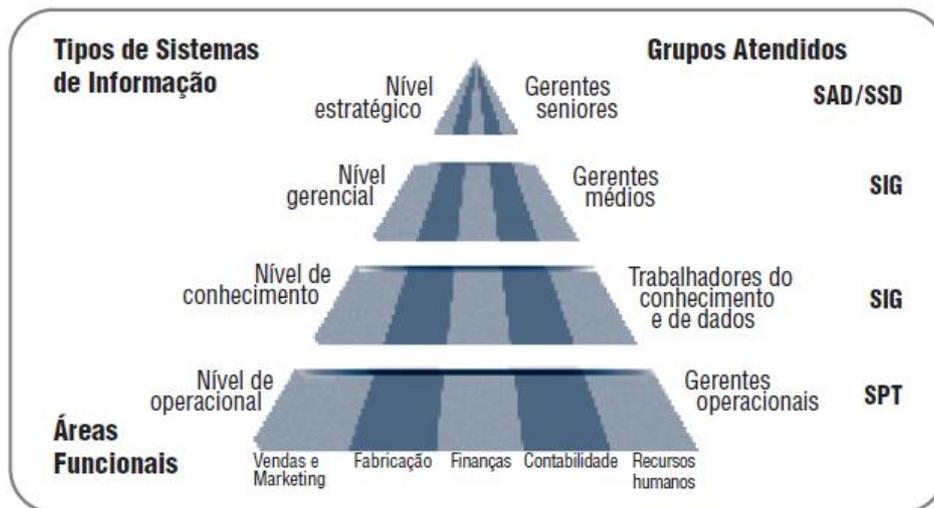


Figura 3 - Tipos de Sistemas de Informação x Grupos de Usuários Atendidos.

2.1. Sistema Processamento de Transação (SPT)

Esta categoria de sistemas, que é utilizada atualmente na maioria das organizações, monitora, coleta, armazena, processa e distribui os dados das diversas transações realizadas dentro da empresa, servindo como base para os demais sistemas existentes dentro da mesma.

Esses sistemas são considerados de extrema importância para o funcionamento das organizações, pois dão suporte a diversas operações do tipo chão-de-fábrica e frente-de-loja, como também são essenciais para suportar as atividades de interface, envolvendo atividades tais como: gestão de materiais, faturamento, elaboração de folha de pagamento, entre outras. Toda vez que a empresa produz ou presta um serviço, ocorre uma transação que será processada por um ou mais SPT's.

O objetivo principal deste tipo de sistema é o fornecimento de todas as informações legais ou organizacionais referentes à empresa, para manter eficientemente os seus negócios. As principais vantagens de utilização deste tipo de sistema são a precisão e confiabilidade obtidas, redução no custo e tempo de obtenção das informações.

Tais sistemas normalmente processam um grande volume de dados para funções rotineiras e, desta forma, são elaborados para suportar o alto grau de repetição do processo, a realização de operações simples, a necessidade de grande capacidade de armazenamento e, por fim, o impacto sobre um grande número de funcionários.

2.2. Sistema de Informação Gerencial (SIG)

A ênfase dos SIG's está sobretudo na saída das informações. Esses sistemas extraem as informações de base de dados compartilhada e de processos que estão de acordo com o que o SIG necessita para suas operações. Cumpre informar, entretanto, que estes dados são originários dos SPT's. Segundo Oliveira (1998), após a coleta dos dados e a transformação dos mesmos em informação, ele tem como principal função prover o gerente com informações passadas e presentes sobre as operações internas e sobre o ambiente da empresa, orientando assim a execução do processo decisório e, paralelamente, assegurando que as estratégias do negócio sejam implementadas fazendo com que os objetivos traçados sejam alcançados de modo satisfatório. O SIG influencia as diferentes áreas funcionais dentro da organização, no nível gerencial, reunindo informações pertinentes a cada uma delas.

As saídas de um SIG envolvem relatórios de natureza variada, sendo os principais listados a seguir:

- Relatórios Programados – Contêm dados rotineiros, que são frequentemente solicitados pela gerencia, com informações sintéticas.
- Relatórios de Pontos Críticos – Visam exibir apenas situações que estão fora dos parâmetros normais, a exemplo de itens de estoque que estão abaixo do ponto mínimo para reposição ou produtos cuja data de validade está próxima do vencimento.
- Relatórios Ad hoc – São documentos concebidos sob demanda, implicam na possibilidade do sistema oferecer facilidades para que sejam criadas novas consultas a partir de novas necessidades dos gerentes.

Enquanto o SPT tem a visão da organização a partir de cada operação com cada cliente (interno ou externo à organização), o SIG busca agregar os dados de determinada operação, fornecendo informações consolidadas sobre aquela operação num determinado período de tempo, para que o gerente tenha um panorama global inerente àquele tipo de operação.

2.3. Sistema de Apoio à Decisão (SAD)

Estes sistemas têm como essência o tratamento de situações onde os problemas são semi-estruturados ou não-estruturados. Embora os SAD's sejam concebidos para atender aos níveis estratégicos, onde problemas desta natureza são mais freqüentes, estes podem servir para toda a organização, pois todos os níveis defrontam-se com problemas pouco- estruturados.

Os SAD's apresentam como suas principais características o uso de dados de diferentes fontes, preocupação com o estilo do decisório e possibilidades de simulação. Tal preocupação, ou estilo cognitivo, é importante, uma vez que as formas de percepção dos dados e a formulação do conhecimento diferem para cada pessoa.

São exemplos de características destes sistemas:

- Manipulação de grande volume de dados – A análise de longas séries históricas de dados é essencial para apoiar análises e decisões eficazes;
- Obter e processar dados de fontes diversas – Os SAD's necessitam de um grande volume de dados que é retirado a partir de sistemas distintos e de fontes externas e internas, a sua eficiência depende desta capacidade de conexão;
- Flexibilidade de relatórios e apresentações – Para representar de forma condensada grande volume de informações, os relatórios devem permitir representações gráficas e textuais, assim como manipulações de detalhamento ou generalizações dos dados, conforme necessidade do executivo;
- Análise de simulações por metas – Consiste em permitir ao usuário a criação de cenários hipotéticos, visando construir projeções de novas situações de negócio. Estas simulações utilizam dentre outros, modelos matemáticos e estatísticos.
- Suporte a abordagens de otimização, satisfação e heurística – As abordagens de otimização correspondem ao emprego de modelos matemáticos determinísticos e estruturados onde a resposta é facilmente encontrada. A abordagem de satisfação envolve problemas semiestruturados e modelos de solução probabilísticos onde não existe um valor único e sim uma faixa de valores que tem a probabilidade de ocorrer. Nas abordagens de heurística temos problemas não-estruturados, com grande complexidade onde o sistema pode encontrar uma boa solução, mas não a melhor.

2.4. Tecnologia por si só não garante segurança da informação

Os dois itens mais importantes no momento de manter as informações da empresa em segurança são: a elaboração de políticas de segurança e o gerenciamento de suporte adequados, seguido do nível de conscientização dos funcionários.

A política de segurança atribui os direitos e responsabilidades às pessoas que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham. Uma política de segurança também deve prever o que pode ser feito na rede da instituição e o que será considerado inaceitável. Tudo o que descumprir a política de segurança pode ser considerado um incidente de segurança.

Os incidentes de segurança devem ser notificados para os responsáveis pela máquina que originou a atividade e também para os grupos de resposta a incidentes e abusos das redes envolvidas. De modo geral a lista de pessoas/entidades a serem notificadas inclui os responsáveis pela rede que originou o incidente, incluindo o grupo de segurança e abusos, se existir um

para aquela rede, bem como o grupo de segurança e abusos da rede em que o usuário está conectado, seja um provedor, empresa, universidade, etc.

3. Uso das Normas

Normas são entendidas como um conjunto de regras ou orientações que visam qualidade, na atuação de uma tarefa. As normas em estudo buscam tornar o ambiente computacional das empresas mais seguro com relação a mitigar os incidentes computacionais, além de orientar sobre ações a serem tomadas, quando estes incidentes ocorrerem.

Aplicar normas de segurança em um ambiente computacional é mais do que modismo, é uma forma de garantir a existência de coerência nas ações dos coordenadores e executores das tarefas de administração dos ambientes computacionais. Adotar padrões reconhecidamente eficientes minimiza-se problemas de incidentes relacionados às operações sustentadas por computadores.

3.1. Entendendo a ABNT NBR ISO/IEC 27002

Segurança para sistemas de informações foi um dos primeiros itens a definirem padrões. A gerência de segurança da informação visa identificar os riscos e implantar medidas que de forma efetiva tornem estes riscos gerenciáveis e minimizados.

A NBR ISO 27002 é um código de práticas de gestão de segurança da informação. Sua importância pode ser dimensionada pelo número crescente de pessoas e variedades de ameaças a que a informação é exposta na rede de computadores.

3.2. Objetivos da Norma

O principal objetivo da Norma é estabelecer um referencial para as organizações desenvolverem, implementarem e avaliarem a gestão da segurança de informação. Em sua documentação a norma aborda 11 tópicos principais:

1. **Política de segurança** - onde descreve a importância e relaciona os principais assuntos que devem ser abordados numa política de segurança.
2. **Segurança organizacional** - aborda a estrutura de uma gerência para a segurança de informação, assim como aborda o estabelecimento de responsabilidades incluindo terceiros e fornecedores de serviços.
3. **Classificação e controle de ativos de informação** - trabalha a classificação, o registro e o controle dos ativos da organização.
4. **Segurança em pessoas** - tem como foco o risco decorrente de atos intencionais ou acidentais feitos por pessoas. Também é abordada a inclusão de responsabilidades relativas à segurança na descrição dos

- cargos, a forma de contratação e o treinamento em assuntos relacionados à segurança.
5. **Segurança ambiental e física** - aborda a necessidade de se definir áreas de circulação restrita e a necessidade de proteger equipamentos e a infra-estrutura de tecnologia de Informação.
 6. **Gerenciamento das operações e comunicações** - aborda as principais áreas que devem ser objeto de especial atenção da segurança. Dentre estas áreas destacam-se as questões relativas a procedimentos operacionais e respectivas responsabilidades, homologação e implantação de sistemas, gerência de redes, controle e prevenção de vírus, controle de mudanças, execução e guarda de backup, controle de documentação, segurança de correio eletrônico, entre outras.
 7. **Controle de acesso** - aborda o controle de acesso a sistemas, a definição de competências, o sistema de monitoração de acesso e uso, a utilização de senhas, dentre outros assuntos.
 8. **Desenvolvimento e manutenção de sistemas** - são abordados os requisitos de segurança dos sistemas, controles de criptografia, controle de arquivos e segurança do desenvolvimento e suporte de sistemas.
 9. **Gestão de incidentes de segurança** - incluída na versão 2005, apresenta dois itens: Notificação de fragilidades e eventos de segurança da informação e gestão de incidentes de segurança da informação e melhorias.
 10. **Gestão da continuidade do negócio** - reforça a necessidade de se ter um plano de continuidade e contingência desenvolvido, implementado, testado e atualizado.
 11. **Conformidade** - aborda a necessidade de observar os requisitos legais, tais como a propriedade intelectual e a proteção das informações de clientes.

4. Norma ABNT NBR ISO/IEC-27001

A norma ABNT NBR ISO/IEC 27001:2005 relaciona os requisitos mandatórios na definição do escopo do Sistema de Gestão da Segurança da Informação, a avaliação de riscos, a identificação de ativos e a eficácia dos controles implementados.

Esta Norma promove a adoção de uma abordagem de processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI - Sistema de Gerenciamento da Segurança da Informação, de uma organização. Para esta abordagem, a norma orienta à observação de um conjunto de ações e tarefas. Estas ações devem ser planejadas visando à eficiência de sua aplicação.

4.1. Entendendo a NBR 27001

A abordagem de processo para a gestão da segurança da informação apresentada nesta norma encoraja que seus usuários enfatizem a importância de:

- Entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança da informação;
- Implantação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;
- Monitoração e análise crítica do desempenho e eficácia do SGSI;
- Melhoria contínua baseada em medições objetivas.

Administrar ambientes computacionais implica em atender as normas e diretrizes da organização. A não conformidade às normas ou o descumprimento ou a não observância implica em penalização legal por omissão a estas. A alegação de desconhecimento não tem valor legal.