Como tratar a Segurança da Informação na organização?

Gestão da Tecnologia da Informação

- Mapear o ambiente (**dimensão**);
- Identificar o que deve ser protegido (**ativo**);
- Estimar o valor do que deverá ser protegido (**valor/risco/impacto**);
- Identificar os envolvidos (**relacionamentos**);
- Definir responsabilidades (**dono da informação/super usuários**);

Gestão da Tecnologia da Informação

- Definir as ações de proteção (**definições**);
- Orçar e adquirir os recursos necessários (**custos**);
- Aplicar as ações e procedimentos (**melhores práticas**);
- Medir os resultados (**monitoramento**);
- Revisão (**processos**).

Conceito de Segurança da Informação

Toda ação ou política relacionada com a proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo, grupo ou uma organização como um todo.

Conceito de Segurança da Informação

É a proteção de dados ou informações: armazenados, em processamento ou em trânsito.

Esta proteção deverá abranger também os recursos humanos, a documentação/material e as áreas/instalações.

Sistema de Gestão da Segurança da informação

SGSI

Conceito SGSI

“Parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.”

(Norma ABNT NBR ISO/IEC 27001).

Normas da Segurança da Informação

ISO/IEC 27000: Sistema de Gestão de Segurança da Informação – Linhas gerais e vocabulário.

ISO/IEC 27001: Sistema de Gestão de Segurança da Informação – Requisitos.

ISO/IEC 27002: Boas práticas para controles de segurança da informação.

ISO/IEC 27003: Guia de implantação do Sistema de Gestão de Segurança da Informação.

ISO/IEC 27004: Gestão da segurança da informação – Medição.

Normas da Segurança da Informação

ISO/IEC 27005: Gestão de risco em segurança da informação.

ISO/IEC 27006: Requisitos para empresas de auditoria e certificação de Sistemas de Gestão de Segurança da Informação.

ISO/IEC 27007: Diretrizes para auditoria em Sistemas de Gestão de Segurança da Informação.

ISO/IEC TR 27008: Diretrizes para auditores sobre controle de segurança da informação.

ISO/IEC 27010: Gestão de segurança da informação para comunicação intersetorial e interorganizacional.

Normas da Segurança da Informação

ISO/IEC 27011: Diretrizes para gestão de segurança da informação em organizações de telecomunicação com base na ISO/IEC 27002.

ISO/IEC 27013: Diretrizes para a implementação integrada da ISO/IEC 27001 e ISO/IEC 20000-1.

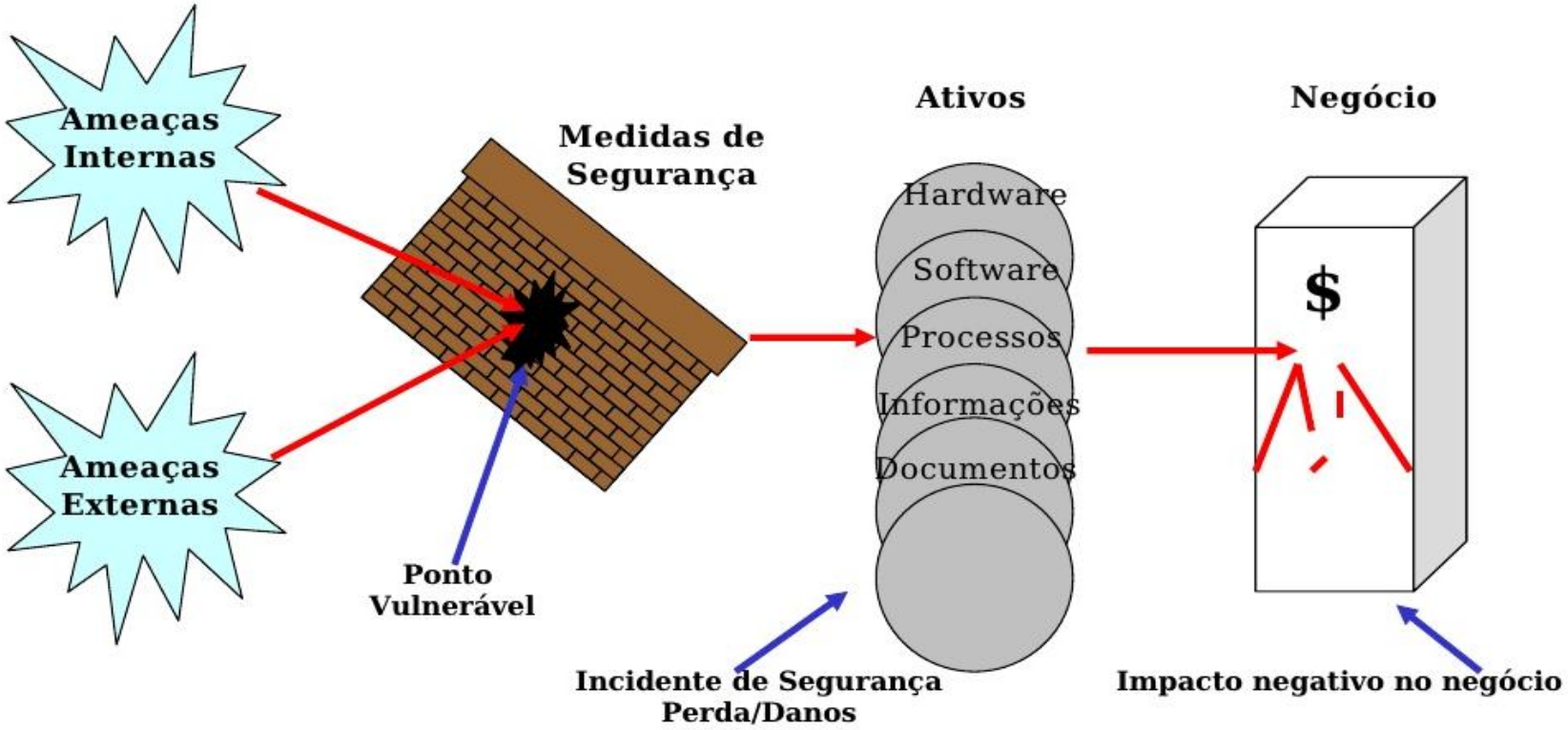
ISO/IEC 27014: Governança de segurança da informação.

ISO/IEC TR 27015: Diretrizes para a gestão de segurança da informação em serviços financeiros.

ISO/IEC TR 27016: Diretrizes para a gestão de segurança da informação – Empresas de economia.

Gestão da Tecnologia da Informação

Ambiente das organizações



Fonte: ProfiscoRS

Conceito de Ameaça

- É um ataque potencial a um ativo da informação.

- É um agente interno/externo que, aproveitando-se da vulnerabilidade, poderá quebrar um ou mais dos aspectos básicos de segurança da informação.

Exemplos de ameaça

- Físicas: Incêndio, inundação, queda de energia, etc.
- Tecnológicas: Bugs de software, defeitos, invasões web, etc.
- Humanas: Erro humano, fraude, descuido, sabotagem, etc.

Conceito de Vulnerabilidade

- É um ponto fraco de um ativo.

- Os ativos de informação possuem vulnerabilidades ou fraquezas que podem gerar, intencionalmente ou não, a indisponibilidade, a quebra de confidencialidade ou integridade.

- Uma vulnerabilidade pode vir a ser explorada ou não.

Conceito de Incidente

É a ocorrência de um evento que pode causar interrupções nos processos de negócio em consequência da violação de algum dos aspectos de um sistema de informação.

Exemplos:

- Desastres naturais;
- Greves;
- Qualquer fator que impeça acesso aos sistemas.

Conceito de Ataque

É um incidente de segurança caracterizado pela existência de um agente que busca obter de algum tipo de retorno, atingindo algum ativo de valor.

Conceito de Ativos

Todo e qualquer recurso que dá suporte aos processos de negócio na organização:

Exemplos:

- Físicos: Listagens, cofre, agenda, arquivos, etc;
- Tecnológicos: Servidores, e-mail, notebook, rede, etc;
- Humanos: Funcionários e terceiros.

Conceito de Impacto

- Um incidente de segurança é medido pelas consequências que possam causar aos processos.

- Ativos possuem valores diferentes, quanto maior for o valor do ativo, maior será o impacto de um eventual incidente que possa ocorrer.

Principais Impactos

- Quebra de sigilo
- Vazamento de informações
- Indisponibilidade dos serviços
- Danos a imagem
- Fraudes.

Conceito de Probabilidade

É a chance de uma falha de segurança ocorrer levando em conta a vulnerabilidade do ativo e as ameaças que venham a explorá-la.

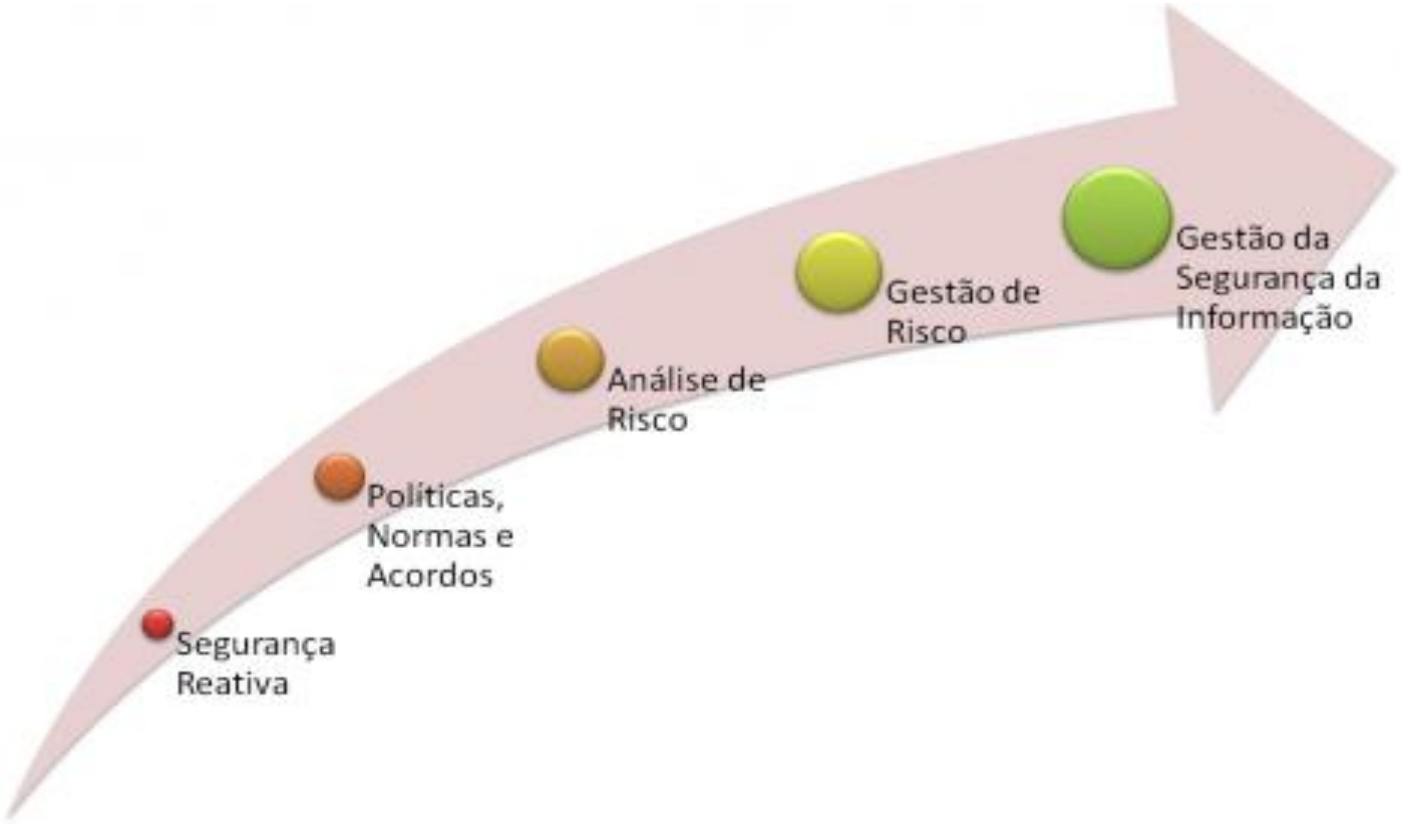
Exemplo de aplicação de controles

- Ativo Físico -> Arquivo para documentos em papel.
- Ameaças -> Cópia ilegal de documentos, fraude, vazamento de informações.
- Vulnerabilidades -> Arquivo sem chave.
- Controles -> Cadeado, Alarme, Guarda.

Fatec Mogi das Cruzes

Gestão da Tecnologia da Informação

Níveis de maturidade da Segurança da Informação



Segurança Reativa (ou fase do essencial)

Fase onde a empresa está focada apenas nas soluções de tecnologia, e onde os controles técnicos básicos fundamentais de segurança da informação são implementados, destacando-se os três controles mais difundidos e implementados: backup, anti-malware e firewall.

Políticas, Normas e Acordos (ou fase documental)

Fase onde ocorre um entendimento maior de que a segurança da informação não será administrada apenas com tecnologia; começa-se a perceber a importância do fator humano, jurídico e normativo.

Análise de Risco

Fase que tem o potencial para ser um divisor de águas na gestão da segurança da informação da empresa. A avaliação de risco difere da análise de vulnerabilidade pois leva em consideração a importância do ativo analisado para os processos de negócio e os objetivos da organização.

Gestão do Risco

Fase em que não apenas a implementação de controles para mitigar os riscos identificados na análise de risco, mas também calcular o risco residual e até mesmo permitir que a direção da empresa aceite riscos, ou seja, formalize o conhecimento dos riscos identificados e que não pretende no momento investir recursos na mitigação do risco, mas conviver com o mesmo temporariamente ou indefinidamente.

Gestão da Segurança da Informação

Fase onde se estabelece um Sistema de Gestão de Segurança da Informação (SGSI ou ISMS) baseado em normas da família 27000.

Políticas de Segurança

- Acesso aos sistemas
- Controle de privilégios
- Vírus
- Ambiente de desenvolvimento
- Segurança dos dados
- Segurança de comunicações
- Segurança na administração de pessoas
- Segurança de pessoas
- Segurança física do ambiente
- Administração da segurança da proteção

Fatec Mogi das Cruzes

Gestão da Tecnologia da Informação

Ciclo de vida da Informação em relação à Segurança da Informação