Norma ABNT NBR ISO/IEC 17799:2005

Prof.: Thiago H. Bom Conselho
UNATEC- Rede de Computadores

Objetivo do Apresentação

- Apresentar considerações e levantamentos fundamentais a segurança da informação.
- Apresentar as descrições, características e objetivos dos itens descritos em norma.

Business

Metade das empresas investe incorretamente em segurança

Quinta-feira, 6 de Março de 2003 - 16h54

IDG Now!

Embora os departamentos de segurança da informação de corporações do mundo todo tenham recebido um aumento médio de 5% em seus orçamentos, um estudo do Giga Information Group revela que mais de 50% das empresas investiram em projetos de segurança incorretos e irrelevantes.

Como resultado, no início deste ano, a maioria das companhias americanas e européias, cortou 30% de seu orçamento de tecnologia destinado à segurança para se aproximar do total mais provável a ser investido neste setor em 2003.

Entretanto, segundo Steve Hunt, analista da Giga Information Group, a maioria dos departamentos de segurança de TI estão economizando bastante sob o ponto de vista estratégico e administrativo. Por isso, cortes em curto prazo não poderão ultrapassar a marca dos 5%.

Para uma redução de custos de 10% a 15%, o analista acredita que seria necessário terceirizar tarefas táticas, como o gerenciamento remoto de firewalls.

A pesquisa ainda informa que, antes dos ataques terroristas de 11 de setembro de 2001, apenas 30% entre todas as empresas norte-americanas e européias tinham capacitado uma pessoa para mapear medidas de segurança.

Este ano, o Giga prevê que mais de 90% de todas as organizações nomearão um indivíduo ou um departamento especial para essa tarefa.

Informação Vs Segurança

- Que Informações precisam de segurança?
  - Identidade
  - CPF
  - Endereço residencial
  - Telefone Celular
  - Código da Maleta
  - Senhas
  - Informações Bancarias
  - Senhas pessoais
  - Numero de cartão de credito
  - Rotinas e Horários de trabalho

Informação Vs Segurança

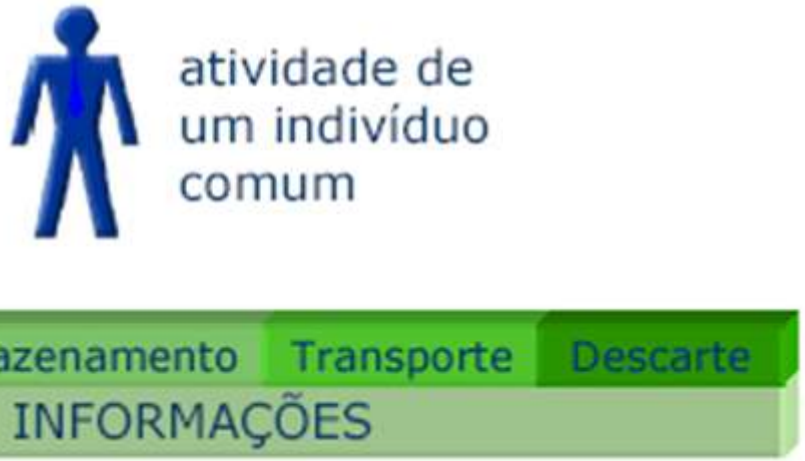
- Por que proteger as informações?
  - Por seu valor
  - Pelo impacto de sua ausência
  - Pelo impacto resultante de seu uso por terceiros
  - Pela importância de sua existência
  - Pela relação de dependência com a sua atividade
  - ...

Informação Vs Segurança

- Quando proteger as informações?

Durante seu ciclo de vida

  - Manuseio
  - Armazenamento
  - Transporte Descarte



Informação Vs Segurança

- Onde proteger as informações?

Nos ativos que as custodiam:

- Físicos
- Tecnológicos
- Humanos

atividade de um indivíduo comum

ATIVOS	FÍSICOS	TECNOLÓGICAS	HUMANOS
	• agenda • sala • arquivo • cofre	• sistema • e-mail • servidor • notebook	• funcionário • parceiro • secretária • porteiro

Informação Vs Segurança

- O que proteger nas informações?

Os conceitos principais:

- Confidencialidade
- Integridade
- Disponibilidade

Os aspectos:

- Legalidade
- Autenticidade

O que podem ser atingidos pela exploração de uma falha ou vulnerabilidade presente em um ativo

VULNERABILIDADES

Informação Vs Segurança

- Do que proteger as Informações?

De ameaças:

- Físicas
- Tecnológicas
- Humanas

atividade de um indivíduo comum

Informação Vs Segurança

atividade de um indivíduo comum

Manuseio | Armazenamento | Transporte | Descarte

INFORMAÇÕES

ATIVOS

FÍSICOS	TECNOLÓGICAS	HUMANOS
• agenda	• sistema	• funcionário
• sala	• e-mail	• parceiro
• arquivo	• servidor	• secretária
• cofre	• notebook	• porteiro

VULNERABILIDADES

AMEAÇAS

FÍSICAS	TECNOLÓGICAS	HUMANAS
• incêndio	• vírus	• sabotagem
• inundação	• bug software	• fraude
• curto circuito	• defeito técnico	• erro humano
• apagão	• invasão web	• descuido

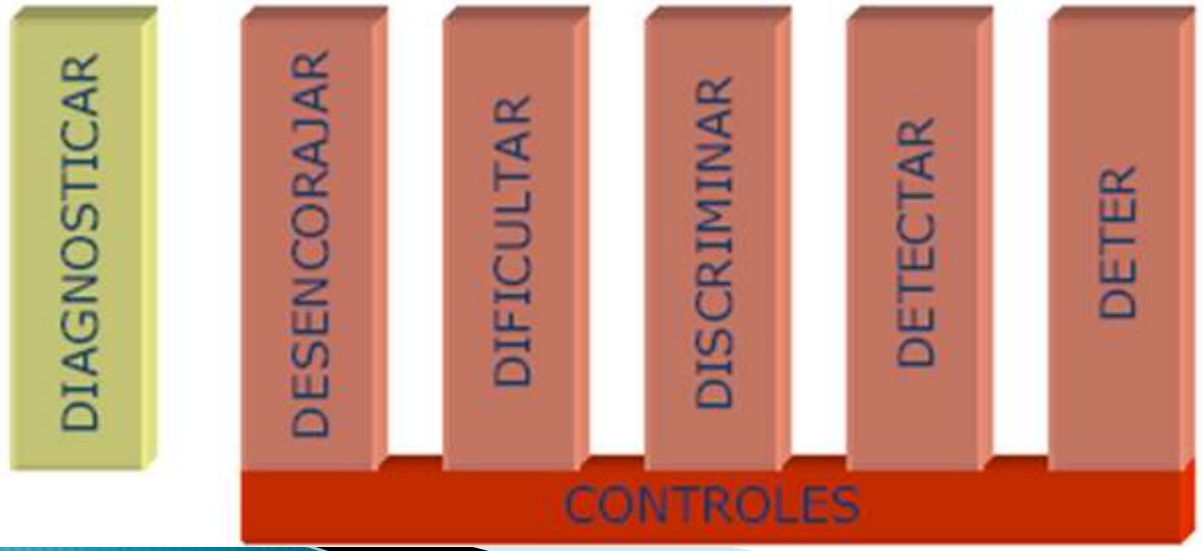
Risco

- **AMEAÇAS** exploram **VULNERABILIDADES** presentes nos **ATIVOS** que mantém informações, causando **IMPACTOS** no negocio.

$$R_{risco} = \frac{\text{Ameaças} \times \text{Vulnerab.} \times \text{Impactos}}{\text{Medidas de Segurança}}$$

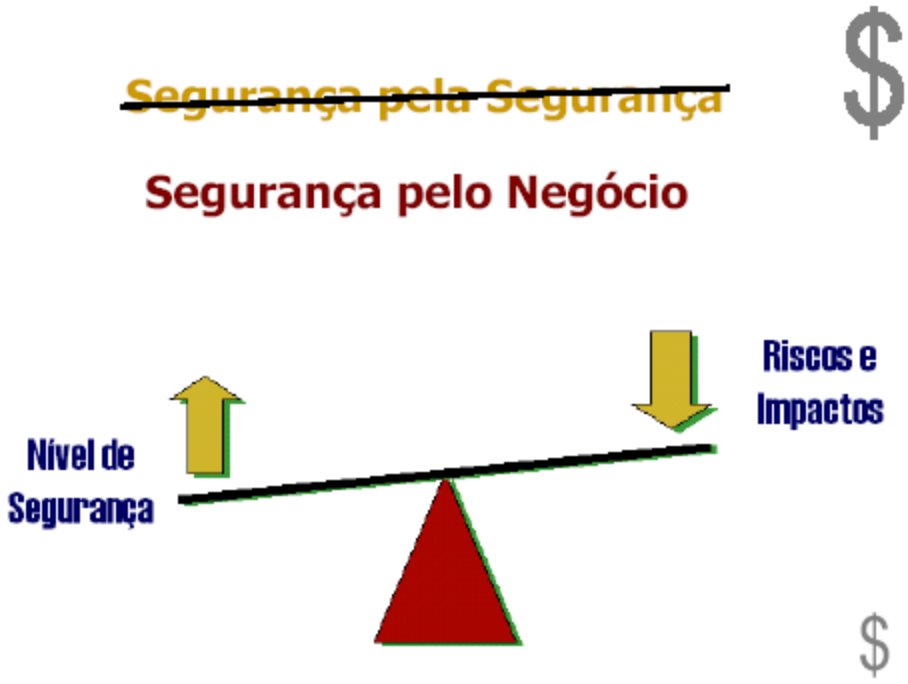
Informação Vs Segurança

- Como proteger as informações?
  - Aplicando controles que eliminem e administrem as vulnerabilidades, reduzindo assim os riscos
  - Segmentando-as pela importância (relevância)
  - Definindo níveis de segurança compatíveis
  - Avaliando o valor da informação e o custo de proteção



Gestão de Risco e Risco de Negocio

- Não existe segurança 100%;
- Segurança é risco tendendo a zero.



Miopia do Iceberg

- Bug de software
- Serviço crítico FTP habilitado
- Desatualização do Sistema Operacional
- Firewall sem configuração devida
- ...
- Alarme e trancas de porta frágil
- Sistema de combate a incêndio inoperante
- Cabeamento desestruturado
- Ausência de controle de acesso físico
- ...
- Email enviado à pessoa errada
- Relatório critico descartado sem cuidado
- Segredo de negócio falado no elevador
- Arquivo eletrônico apagado distraidamente

Por que adotar uma Política de Segurança

- Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado;
- Diminuir ou eliminar a possibilidade de fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação;
- Proteger as infra-estruturas críticas ao negócio;
- Estabelecer procedimentos apropriados;
- Conseguir o compromisso das pessoas envolvidas (funcionários, acionistas, terceiros, fornecedores, clientes, outros);

Compliance: Referências Técnicas

- Código Civil
- ISO 17799, CobiT®, ITIL®, COSO
- Sarbanes Oxley
- CVM 358
- Basiléia 2, Banco Central 2554/2817
- Decreto 4553, Melhores Práticas do TCU
- Norma NBr ISO Guia 73, 4360
- Susep 249, 285
- Projeto de Lei 89 – Crimes por Computador
- Legislação da ICP Brasil
- EUA: FISMA, CIP, HIPPA
- Outras Leis, Resoluções, Decretos, Portarias e Normas

ABNT NBR ISO/IEC 17799:2005

Tecnologia da informação
Técnicas de segurança
Código de prática para a gestão da segurança da informação

Prefácio Nacional

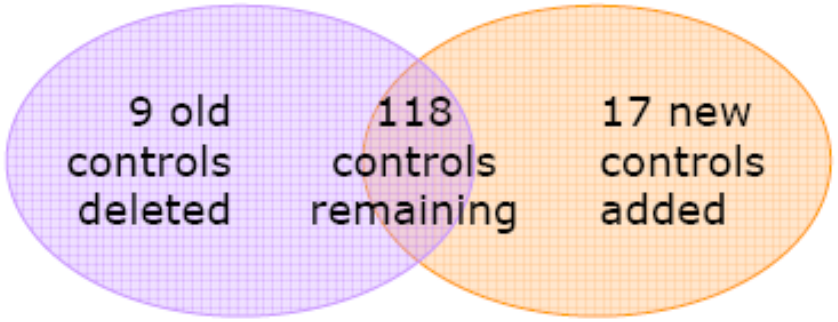
- A Associação Brasileira de Normas Técnicas (ABNT) é o Fórum Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais Temporárias (ABNT/CEET), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).
- A ABNT NBR ISO/IEC 17799 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:204.01). O Projeto circulou em Consulta Nacional conforme Edital nº 03, de 31.03.2005, com o número de Projeto NBR ISO/IEC 17799.
- Esta Norma é equivalente à ISO/IEC 17799:2005.
- Uma família de normas de sistema de gestão de segurança da informação (SGSI) está sendo desenvolvida no ISO/IEC JTC 1/SC 27. A família inclui normas sobre requisitos de sistema de gestão da segurança da informação, gestão de riscos, métricas e medidas, e diretrizes para implementação. Esta família adotará um esquema de numeração usando a série de números 27000 em seqüência.
- A partir de 2007, a nova edição da ISO/IEC 17799 será incorporada ao novo esquema de numeração como ISO/IEC 27002.

ISO/IEC 17799 Revision

2000 edition	2005 edition
Security policy	Security policy
Security organisation	Organising information security
Asset classification & control	Asset management
Personnel security	Human resources security
Physical & environmental security	Physical & environmental security
Communications & operations management	Communications & operations management
Access control	Access control
Systems development & maintenance	Information systems acquisition, development and maintenance
	Information security incident management
Business continuity	Business continuity management
Compliance	Compliance

Control Objectives/Controls

ISO/IEC 17799
old edition



ISO/IEC 17799
new edition

There are *8 new controls objectives* in the revised version of the standard

5 control objectives have been re-arranged into other controls objectives

4. Análise/avaliação e tratamento de riscos

- Controles:
  - 4.1) Analisando/avaliando os riscos de segurança da informação;
  - 4.2) Tratando os riscos de segurança da informação

5. Política de segurança da informação.

- Objetivo: Prover uma orientação e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.
- Controles:
  - 5.1) Política de segurança da informação;
  - 5.1.1) Documentação da política de segurança da informação;
  - 5.1.2) Análise crítica da política de segurança da informação.

5. Política de segurança da informação.

- Qual a afirmativa é mais próxima à Política de Segurança em sua organização:
  - Está atualizada e é seguida pelos usuários
  - É seguida mas não está atualizada
  - É conhecida mas não é seguida pelos usuários
  - Foi publicada mas não é conhecida pelos usuários
  - Foi desenvolvida mas não foi publicada
  - Está em desenvolvimento
  - Não foi desenvolvida

6. Organizando a segurança da informação

- Objetivo: Gerenciar a segurança da informação dentro da organização.
- Controles:
  - 6.1) Infra-estrutura da segurança da informação;
  - 6.1.1) Comprometimento da direção com a segurança da informação;
  - 6.1.2) Coordenação da segurança da informação;
  - 6.1.3) Atribuição de responsabilidades para a segurança da informação.
  - 6.1.4) Processo de autorização para os recursos de processamento da informação;
  - 6.1.5) Acordos de confidencialidade;
  - 6.1.6) Contato com autoridades;
  - 6.1.7)Contato com grupos especiais;
  - 6.1.8) Análise crítica independente de segurança da informação;
  - 6.2)Partes externas;
  - 6.2.1) Identificação dos riscos relacionados com partes externas;
  - 6.2.2) Identificando a segurança da informação, quando tratando com clientes;
  - 6.2.3) Identificando segurança da informação nos acordos com terceiros;

6. Organizando a Segurança da Informação

- Quem é o responsável pela Segurança da Informação em seu órgão?
  - O Escritório de Segurança da Informação (Security Officer)
  - A área de TI
  - A área de Redes
  - Auditoria, Gestão de Riscos, Compliance ou outras
  - Não existe responsabilidade formal

7. Gestão de ativos

- Objetivo: Alcançar e manter a proteção adequada dos ativos da organização.
- Controles:
  - 7.1) Responsabilidade pelos ativos;
  - 7.1.1) Inventário dos ativos;
  - 7.1.2) Proprietário dos ativos;
  - 7.1.3) Uso aceitável dos ativos;
  - 7.2) Classificação da informação;
  - 7.2.1) Recomendações parar classificação;
  - 7.2.2) Rótulos e tratamento da informação.

7. Gestão de Ativos

- Quanto aos ativos de sua organização (pessoas, processos, sistemas e equipamentos):
  - Estão inventariados e analisados em toda a organização
  - Estão inventariados em toda a organização mas não foram analisados
  - Estão inventariados e analisados nos escopos mais importantes
  - Estão inventariados nos escopos mais importantes mas não foram analisados
  - Não estão inventariados

8. Segurança em recursos humanos

- Objetivo: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos.
- Controles:
  - 8.1) Antes da Contratação;
  - 8.1.1) Papéis e responsabilidades;
  - 8.1.2) Seleção;
  - 8.1.3) Termos e condições de contratação;
  - 8.2) Durante a contratação;
  - 8.2.1) Responsabilidades da direção;
  - 8.2.2) Concientização, educação e treinamento em segurança da informação;
  - 8.2.3) Processo disciplinar;
  - 8.3) Encerramento ou mudança da contratação;
  - 8.3.1) Encerramento de atividades;
  - 8.3.2) evolução de ativos;
  - 8.3.3) Retirada de direitos de acesso;

8. Segurança em Recursos Humanos

- Qual o grau de conscientização dos gestores usuários em Segurança da Informação:
  - Baixa
  - Média
  - Alta

9. Segurança física e do ambiente

- Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.
- Controles:
  - 9.1) Áreas seguras
  - 9.1.1) Perímetro de segurança;
  - 9.1.2) Controles de entrada física;
  - 9.1.3) Segurança em escritórios, salas e instalações;
  - 9.1.4) Proteção contra ameaças externas e do meio ambiente;
  - 9.1.5) Trabalhando em áreas seguras;
  - 9.1.6) Acesso do público, áreas de entrega e de carregamento;
  - 9.2) Segurança de equipamentos;
  - 9.2.1) Instalação e proteção do equipamento;
  - 9.2.2) Utilidades;
  - 9.2.3) Segurança do cabeamento;
  - 9.2.4) Manutenção dos equipamentos;
  - 9.2.5) Segurança de equipamentos fora das dependências da organização;
  - 9.2.6) Reutilização e alienação segura de equipamentos;
  - 9.2.7) Remoção de propriedade;

9. Segurança Física e do Ambiente

- Quanto à segurança física dos equipamentos compartilhados (servidores, bancos de dados, …):
  - Ficam em salas convencionais junto com os backups;
  - Ficam em salas convencionais e os backups são armazenados for a da organização;
  - Ficam em salas preparadas junto com os backups;
  - Ficam em salas preparadas e os backups são armazenados for a da organização;
  - Ficam em uma sala cofre.

10. Gerenciamento das operações e comunicações

- Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.
- Controles:
  - 10.1) Procedimentos e responsabilidades operacionais;
  - 10.1.1) Documentação dos procedimentos de operação;
  - 10.1.2) Gestão de mudanças;
  - 10.1.3) Segregação de funções;
  - 10.1.4) Separação dos recursos de desenvolvimento, teste e de produção;
  - 10.2) Gerenciamento de serviços terceirizados;
  - 10.2.1) Entrega de serviços;
  - 10.2.2) Monitoramento e análise crítica de serviços terceirizados;
  - 10.2.3) Gerenciamento de mudanças para serviços terceirizados;
  - 10.3) Planejamento e aceitação dos sistemas;
  - 10.3.1) Gestão de capacidade;
  - 10.3.2) Aceitação de sistemas;
  - 10.4) Proteção contra códigos maliciosos e códigos móveis;
  - 10.4.1) Controles contra códigos maliciosos;
  - 10.4.2) Controles contra códigos móveis;
  - 10.5) Cópias de segurança;
  - 10.5.1) Cópias de segurança da informação;
  - 10.6) Gerenciamento da segurança em redes;
  - 10.6.1) Controles de redes;
  - 10.6.2) Segurança dos serviços de redes;

10. Continuação

- 10.7) Manuseio de mídias;
- 10.7.1) Gerenciamento de mídias removíveis;
- 10.7.2) Descarte de mídias;
- 10.7.3) Procedimentos para tratamento de informação;
- 10.7.4) Segurança da documentação dos sistemas;
- 10.8) Troca de informações;
- 10.8.1) Políticas e procedimentos para a troca de informações;
- 10.8.2) Acordos para a troca de informações;
- 10.8.3) Mídias em trânsito;
- 10.8.4) Mensagens eletrônicas;
- 10.8.5) Sistemas de informação do negócio;
- 10.9) Serviços de comércio eletrônico;
- 10.9.1) Comércio eletrônico;
- 10.9.2) Transações on-line;
- 10.9.3) Informações publicamente disponíveis;
- 10.10) Monitoramento;
- 10.10.1) Registros de auditoria;
- 10.10.2) Monitoramento do uso de sistema;
- 10.10.3) Proteção das informações dos registros (log);
- 10.10.4) Registros (log) de administrador e operador;
- 10.10.5) Registros (log) de falhas;
- 10.10.6) Sincronização dos relógios;

10. Gerenciamento das Operações e Comunicação

- Quanto aos procedimentos de segurança no ambiente técnico, podemos afirmar:
  - Que existe um modelo de análise e gestão de riscos implementado no ambiente de tecnologia da informação;
  - Que existe um modelo de análise e gestão de riscos implementado nos ambientes mais críticos;
  - Que a ação é feita em resposta aos acontecimentos.

11. Controle de acessos

- Objetivo: Controlar o acesso à informação.
- Controles:
  - 11.1) Requisitos de negócio para controle de acesso;
  - 11.1.1) Política de controle de acesso;
  - 11.2) Gerenciamento de acesso do usuário;
  - 11.2.1) Gerenciamento de privilégios;
  - 11.2.2) Gerenciamento de senha do usuário;
  - 11.2.3) Análise crítica dos direitos de acesso de usuário;
  - 11.3) Responsabilidade dos usuários;
  - 11.3.1) Uso de senhas;
  - 11.3.2) Equipamento de usuário sem monitoração;
  - 11.3.3) Política de mesa limpa e tela limpa;
  - 11.4) Controle de acesso à rede;
  - 11.4.1) Política de uso dos serviços de rede;
  - 11.4.2) Autenticação para conexão externa do usuário;
  - 11.4.3) Identificação de equipamento em redes;
  - 11.4.4) Proteção e configuração de portas de diagnóstico remotas;
  - 11.4.5) Segregação de redes;
  - 11.4.6) Controle de conexão de rede;
  - 11.4.7) Controle de roteamento de redes;

11. Continuação

- 11.5) Controle de acesso ao sistema operacional;
- 11.5.1) Procedimentos seguros de entrada no sistema (log-on);
- 11.5.2) Identificação e autenticação de usuário;
- 11.5.3) Sistema de gerenciamento de senha;
- 11.5.4) Uso de utilitários de sistema;
- 11.5.5) Desconexão de terminal por inatividade;
- 11.5.6) Limitação de horário de conexão;
- 11.6) Controle de acesso à aplicação e à informação;
- 11.6.1) Restrição de acesso à informação;
- 11.6.2) Isolamento de sistemas sensíveis;
- 11.7) Computação móvel e trabalho remoto;
- 11.7.1) Computação e comunicação móvel;
- 11.7.2) Trabalho remoto;

11. Controle de Acessos

- Quanto ao uso de senhas em sua organização:
  - Existe uma política formal e senhas fortes;
  - Não existe uma política formal, mas os usuários estão conscientizados;
  - Não existe uma política formal.

12. Aquisição, desenvolvimento e manutenção de sistemas de informação

- Objetivo: Garantir que segurança é parte integrante de sistemas de informação.
- Controles:
  - 12.1) Requisitos de segurança de sistemas de informação;
  - 12.1.1) Análise e especificação dos requisitos de segurança;
  - 12.2) Processamento correto nas aplicações;
  - 12.2.1) Validação dos dados de entrada;
  - 12.2.2) Controle do processamento interno;
  - 12.2.3) Integridade de mensagens;
  - 12.2.4) Validação de dados de saída;
  - 12.3) Controles criptográficos;
  - 12.3.1) Política para o uso de controles criptográficos;
  - 12.3.2) Gerenciamento das chaves;
  - 12.4) Segurança dos arquivos do sistema;
  - 12.4.1) Controle de software operacional;
  - 12.4.2) Proteção dos dados para teste de sistema;
  - 12.4.3) Controle de acesso ao código-fonte de programa;
  - 12.5) Segurança em processos de desenvolvimento e de suporte;
  - 12.5.1) Procedimentos parar controle de mudanças;
  - 12.5.2) Análise crítica técnica das aplicações após mudanças n sistema operacional;
  - 12.5.3) Restrições sobre mudanças em pacotes de software;
  - 12.5.4) Vazamento de informações;
  - 12.5.5) Desenvolvimento de terceirizado de software;
  - 12.6) Gestão de vulnerabilidades técnicas;
  - 12.6.1) Controle de vulnerabilidades técnicas;

12. Aquisição, desenvolvimento e manutenção de sistemas

- Quanto a segurança nos sistemas:
  - Existem procedimentos formalizados;
  - São realizadas análises periódicas conforme o conhecimento da equipe técnica;
  - Não existem procedimentos formalizados e a equipe técnica necessita aumentar seus conhecimentos;

13. Gestão de incidentes de segurança da informação

- Objetivo: Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.
- Controles:
  - 13.1) Notificação de fragilidades e eventos de segurança da informação;
  - 13.1.1) Notificação de eventos de segurança da informação;
  - 13.1.2) Notificando fragilidades de segurança da informação;
  - 13.2) Gestão de incidentes de segurança da informação e melhorias;
  - 13.2.1) Responsabilidades e procedimentos;
  - 13.2.2) Aprendendo com os incidentes de segurança da informação;
  - 13.2.3) Coleta de evidências;

13. Gestão de Incidentes de Segurança da Informação

- Como é feita a notificação de incidentes?
  - Existe um sistema e procedimentos formalizados;
  - Existe uma pessoa/departamento responsável;
  - Não está formalizado.

14. Gestão da continuidade do negócio

- Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.
- Controles:
  - 14.1) Aspectos da gestão da continuidade do negócio, relativos à segurança da informação;
  - 14.1.1) Incluindo segurança da informação no processo de gestão da continuidade de negócio;
  - 14.1.2) Continuidade de negócios e análise/ avaliação de riscos;
  - 14.1.3) Desenvolvimento e implantação de planos de continuidade relativos à segurança da informação;
  - 14.1.4) Estrutura do plano de continuidade do negócio;
  - 14.1.5) Testes, manutenção e reavaliação dos planos de continuidade do negócio;

14. Gestão da Continuidade do Negócio

- Qual a afirmativa é mais próxima ao Plano de Continuidade dos Negócios?
  - É conhecido e está atualizado;
  - É conhecido mas não está atualizado;
  - Foi publicado mas não é conhecido pelos usuários;
  - Foi desenvolvido mas não foi publicado;
  - Está em desenvolvimento;
  - Não foi desenvolvido.

15. Conformidade

- Objetivo: Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
- Controles:
  - 15.1) Conformidade com requisitos legais;
  - 15.1.1) Identificação da legislação vigente;
  - 15.1.2) Direitos de propriedade intelectual;
  - 15.1.3) Proteção de registros organizacionais;
  - 15.1.4) Proteção de dados e privacidade de informações pessoais;
  - 15.1.5) Prevenção de mau uso de recursos de processamento da informação;
  - 15.1.6) Regulamentação de controles de criptografia;
  - 15.2) Conformidade com normas e políticas de segurança da informação e conformidade técnica;
  - 15.2.1) Conformidade com as políticas e normas de segurança da informação;
  - 15.2.2) Verificação da conformidade técnica;
  - 15.3) Considerações quanto à auditoria de sistemas de informação;
  - 15.3.1) Controles de auditoria de sistemas de informação;
  - 15.3.2) Proteção de ferramentas de auditoria de sistemas de informação;

15. Conformidade

- Quanto as publicações legais e regulamentares, sua organização:
  - Conhece as publicações que a organização deve seguir e a responsabilidade dos administradores e técnicos;
  - Conhece as publicações que sua organização deve seguir, mas não conhece a responsabilidade dos administradores e técnicos;
  - Conhece as publicações e responsabilidades em parte;
  - Não conhece as publicações que a organização deve seguir.

10 Fatores Críticos de Sucesso

- 1. Trate a segurança de forma integrada;
- 2. Considere o Trinômio: Tecnologia, Processos e Pessoas;
- 3. Não perca as necessidades do negocio de vista;
- 4. Persiga continuamente o ROI da Segurança [Custo x Beneficio];
- 5. Defina métricas de segurança próprias para o negocio;
- 6. Construa um modelo dinâmico de acompanhamento de índices;
- 7. Adote a norma como guia de orientação;
- 8. Lembre-se que nem todos os controles são aplicáveis;
- 9. Siga o modelo PDCA [Plan, DO, Check, ACT]
- 10. Certificação deverá ser o resultado de um bom trabalho.

Conclusão

- Vamos pensar um pouco?!?

Bibliografia e Complementos

- Proteger as informações e assegurar a continuidade do negócio de nossos clientes, Maximilian Immo Orm Gorissen
- ABNT NBR ISO/IEC 17799:2005, ABNT