Introdução à Segurança da Informação

Plano Continuidade de Negócio: Planos de Contingência

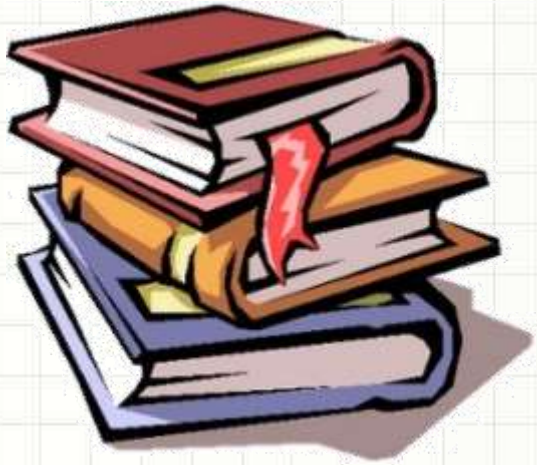
Prof. Dr. Daniel Caetano

2020 - 1

Objetivos

- Compreender o que é a e importância de um Plano de Continuidade de Negócios
- Conhecer as fontes de informação para a elaboração de um Plano de Contingência
- Conhecer os elementos que fazem parte de um Plano de Contingência
- Tomar contato com os conceitos das normas de segurança nacionais.

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 10)
Material Didático	Gestão de Segurança da Informação, Cap 5.6.
Leitura Adicional	http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf (Cartilha do TCU) - Cap. 3

Retomando o Contexto:

Importância da Informação

Importância da Informação

- Informações são um **ativo** da empresa
  - Devem ser protegidas!
    - Garantir continuidade dos negócios
    - Maximizar o retorno de investimentos/oportunidades
    - Minimizar transtornos.

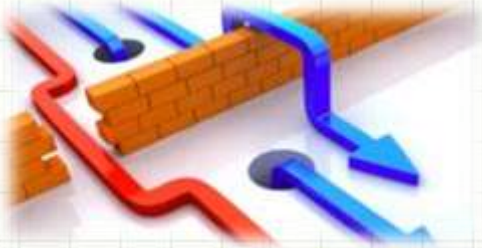
Informação é Essencial

- O mundo mudou muito nas últimas décadas
  - Documentos e processos são digitais: nuvem
  - Todos os dispositivos “sempre online”!

Plano de Continuidade de Negócios

Continuidade de Negócios?

- Informações: essenciais
  - Para a empresa funcionar
- Desastres
  - Podem impedir a continuidade dos negócios!
- Até agora: muitos aspectos de prevenção
  - Alguns conceitos e dicas de recuperação

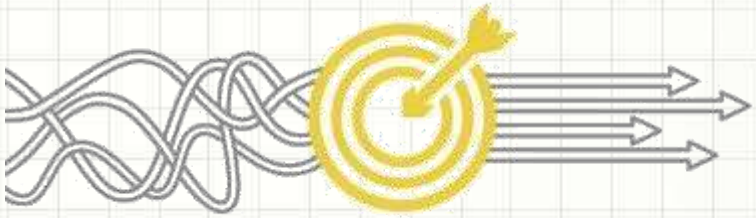


- Como unir tudo?
  - Plano de Continuidade de Negócios (PCN)

Objetivo e Criação do PCN

- Objetivo geral: minimizar impactos
  - Manter a integridade e disponibilidade dos dados
    - Continuar operando em caso de desastre
    - Recuperação ordenada no menor tempo possível.
- Como isso pode ser concretizado?
  - Antever potenciais desastres/catástrofes
  - Planejar solução operacional em cada caso.

Metas de um PCN



- Segurança das pessoas
  - Empregados/colaboradores e visitantes
- Minimizar perdas e danos imediatos
  - Físicas e lógicas
- Rápida restauração das atividades
  - Instalações e equipamentos
- Rápida reativação dos processos críticos
  - Manter o negócio em funcionamento!
- Conscientização e treinamento
  - Responsáveis pela execução do plano!

Insumos para o PCN

- Análise de Risco
  - Identificar todos os desastres possíveis
  - Consequências da interrupção de cada sistema
  - Tempo limite para a recuperação
  - Identificação e priorização
    - Recursos, sistemas, processos críticos...

Insumos para o PCN

- Identificação de Mecanismos de Prevenção
  - No Breaks / Geradores
  - Detectores de incêndio
  - Ar condicionado
  - Cofres à prova de fogo, água e fumaça
  - Armazenagem externa / Backups
  - Criptografia.

Insumos para o PCN

- Estratégias de Recuperação
  - Backups e localidades alternativas
  - Reposição de equipamentos e manutenção (SLA).

Elementos Básicos de um Plano de Contingência

Forma do Plano de Contingência

- Cinco seções
  1. Informação de Suporte
  2. Notificação/Ativação
  3. Recuperação
  4. Reconstituição
  5. Anexos

PC: Informação de Suporte

- Operação
  - Explicação geral e resumida do processo
- Situações de uso
  - Em que situações deve ser acionado
- Sistemas envolvidos
  - Todos os impactados
- Responsáveis
  - Quem cuida de cada sistema envolvido
- Hierarquia de notificação
  - Quem deve acionar quem para a recuperação.

PC: Notificação/Ativação

- Procedimentos Iniciais
  - "Primeiros socorros"
- Processo de Notificação de Responsáveis
  - Ordem, telefone, informações a passar...
- Avaliação de Danos (Processo para)
  - Causa, nível de emergência, áreas afetadas, tipos de danos etc.
- Ativação
  - Como proceder a ativação...
  - ...quando os danos apurados assim exigirem

PC: Recuperação

- Sequência das atividades de recuperação
  - Ordem detalhada dos procedimentos
- Habilitação de Sistemas Alternativos
  - Síntese dos recursos utilizados
  - Procedimento detalhado
- Recuperação do Sistema Principal
  - Métodos (+ de 1? critérios objetivos!)
  - Procedimento detalhado
  - Testes do sistema reconstituído

PC: Reconstituição

- Desmobilização da Contingência
  - Desativação dos sistemas alternativos
  - Reativação dos sistemas restaurados
- Testes dos Sistemas Principais
  - Avaliação da Recuperação
- Integração de Dados
  - Incorporação dos dados de operação...
  - ...do sistema alternativo para o principal.

PC: Anexos

- Responsáveis pelo plano
  - Qualquer informação adicional pertinente
  - Informações sobre serviços externos e SLAs
  - Apoio alternativo em caso de indisponibilidade
- *Checklists*
  - Listas de acompanhamento
- Especificações técnicas
  - Toda inform. útil na recuperação
    - Equipamentos / Software
- …

Requisitos para PCN Funcionar

- Apoio da alta administração
  - Fundamental!
- Treinamento e conscientização
  - Não pode ser novidade na hora do desastre!
- Teste do PCN
  - Evitar pressupostos incorretos, omissões etc.
  - Mudanças!
- Revisões periódicas
  - Ambiente, pessoas, endereços, leis... Tudo muda.

Noções:

Normas NBR ISO/IEC 27001 e ISO/IEC 27002

Norma ISO/IEC 17799:2005

- Diretrizes e princípios para melhorar...
  - ... Gestão de Segurança da Informação da empresa
  - Internacionalização da BS 7799.
- Objetivo:
  - Controles a implementar em função...
  - ...requisitos identificados pela Análise de Risco.
- Norma pode servir como um guia prático
  - Desenvolvimento dos procedimentos de segurança
  - E a elaboração de políticas
- Foi incorporada à ISO/IEC 27002.

Norma ISO/IEC 27002

- Código de Prática para a GSI
  - Gestão de Segurança da Informação

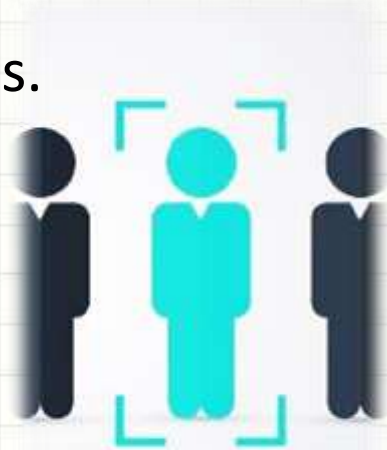
- Objetivo
  - Estabelecer diretrizes e princípios iniciais para:
    - Iniciar, implementar e melhorar a GSI da organização
  - Ou seja: proteger informações importantes...
    - ...para a continuidade dos negócios.

Norma ISO/IEC 27002 - Tópicos

- Política de Segurança da Informação
  - Formalizada em documento e comunicada claramente; deve ser revisada periodicamente
- Organizando a Segurança da Informação
  - Deve haver uma estrutura gerencial envolvendo representantes estratégicos de diversas áreas. Importante estabelecer acordos de sigilo.
- Gestão de Ativos
  - Manter e proteger ativos – identificar, classificar, catalogar etc. de maneira estruturada.

Norma ISO/IEC 27002 - Tópicos

- Segurança em Recursos Humanos
  - Descrições de cargos e termos de contratação devem ser explícitos no que tange às responsabilidades de Segurança da Informação.
  - Candidatos: análise minuciosa!
    - Especial: manuseio de informações sigilosas.
  - Todos: estar cientes das ameaças
    - E de suas responsabilidades e obrigações.
- Segurança Física e do Ambiente
  - Controle rigoroso, com proteção de equipamentos



Norma ISO/IEC 27002 - Tópicos

- Gestão das Operações e Comunicações
  - Procedimentos e responsabilidades operacionais
  - Diretrizes para gerenciamento de terceirizados
  - Diretrizes para segurança em redes e comunicações
- Controles de Acessos
  - Mecanismos do controle e responsabilização
  - Aspectos sobre computação móvel e teletrabalho
  - Passam por políticas e gerenciamento de privilégios

Norma ISO/IEC 27002 - Tópicos

- Aquisição, Desesenv. e Manut. de Sist. de Infor.
  - Definição de requisitos para aplicações
  - Uso de controles criptográficos
  - Diretrizes de segurança de arquivos e desenvolv.
- Gestão de Incidentes de Segurança da Inform.
  - Gestão e comunicação de fragilidades
  - Coleta de evidências e mecanismos de análise

Norma ISO/IEC 27002 - Tópicos

- Gestão da Continuidade do Negócio
  - Diretrizes para prevenir interrupção do negócio
  - Recuperação e retomada em tempo mínimo
- Conformidade
  - Orientações para evitar violações legais
  - Diretrizes para identificar a legislação vigente:
    - Proteção de registros e direitos de P.I.
    - Proteção de dados e inform. pessoais
    - Prevenção de mau uso dos recursos
    - Regulamentação de criptografia

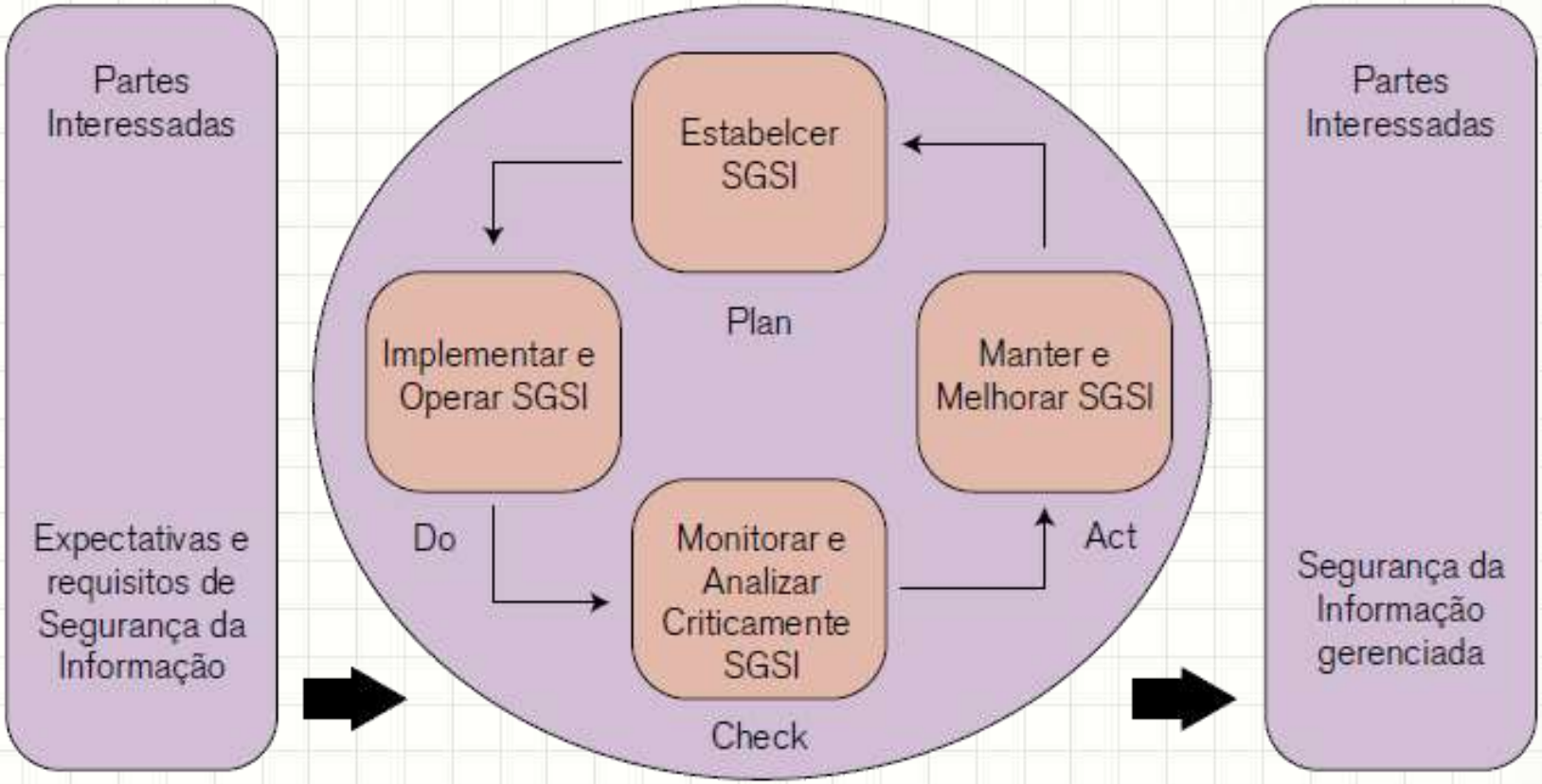
Norma ISO/IEC 27001

- Requisitos para um SGSI
  - Sistema de Gestão de Segurança da Informação
  - Compatível com ISO 9001:2000 e ISO 14001:2004
- Em que se baseia um SGSI?
  - Abordagem de riscos de negócio
- Norma: sugere abordagem de processos
  - Identificar e gerenciar os processos do SGSI
- Ciclo PDCA
  - Plan, Do, Check, Act

https://www.youtube.com/watch?v=2MLmqQaLAFk

Norma ISO/IEC 27001

- Ciclo PDCA na implantação do SGSI



Norma ISO/IEC 27001

- Objetivo: requisitos para quê?
  - Estabelecimento, implementação, operação, monitoração, análise crítica, manutenção e melhoria de um SGSI
- Se aplicam a que tipo de empresas?
  - Quaisquer, independente de tipo, tamanho ou natureza
- Ajuda a proteger ativos de informação
- Única norma auditável para esse fim

Norma ISO/IEC 27001

- Significado da Certificação
  - Requisitos de governança e continuidade de negócios são atendidos
  - Leis e regulamentos aplicáveis são observados
  - Segurança da informação é de suma importância
  - Riscos são corretamente identificados, avaliados e gerenciados
  - Comprometimento da alta gestão
  - Auditorias regulares ajudam na melhoria contínua

QUESTÕES

Quiz

Dois objetivos **muito relevantes** do Plano de Continuidade de Negócios são...

https://kahoot.it/

Conclusões

Resumo e Próximos Passos

- Plano de Continuidade de Negócios
  - ...e os Planos de Contingência
  - Elementos fundacionais
- Conteúdo de um Plano de Contingência
- Noções NBR ISSO/IEC 27001 e 27002

- Preparar-se para as provas!

PERGUNTAS?