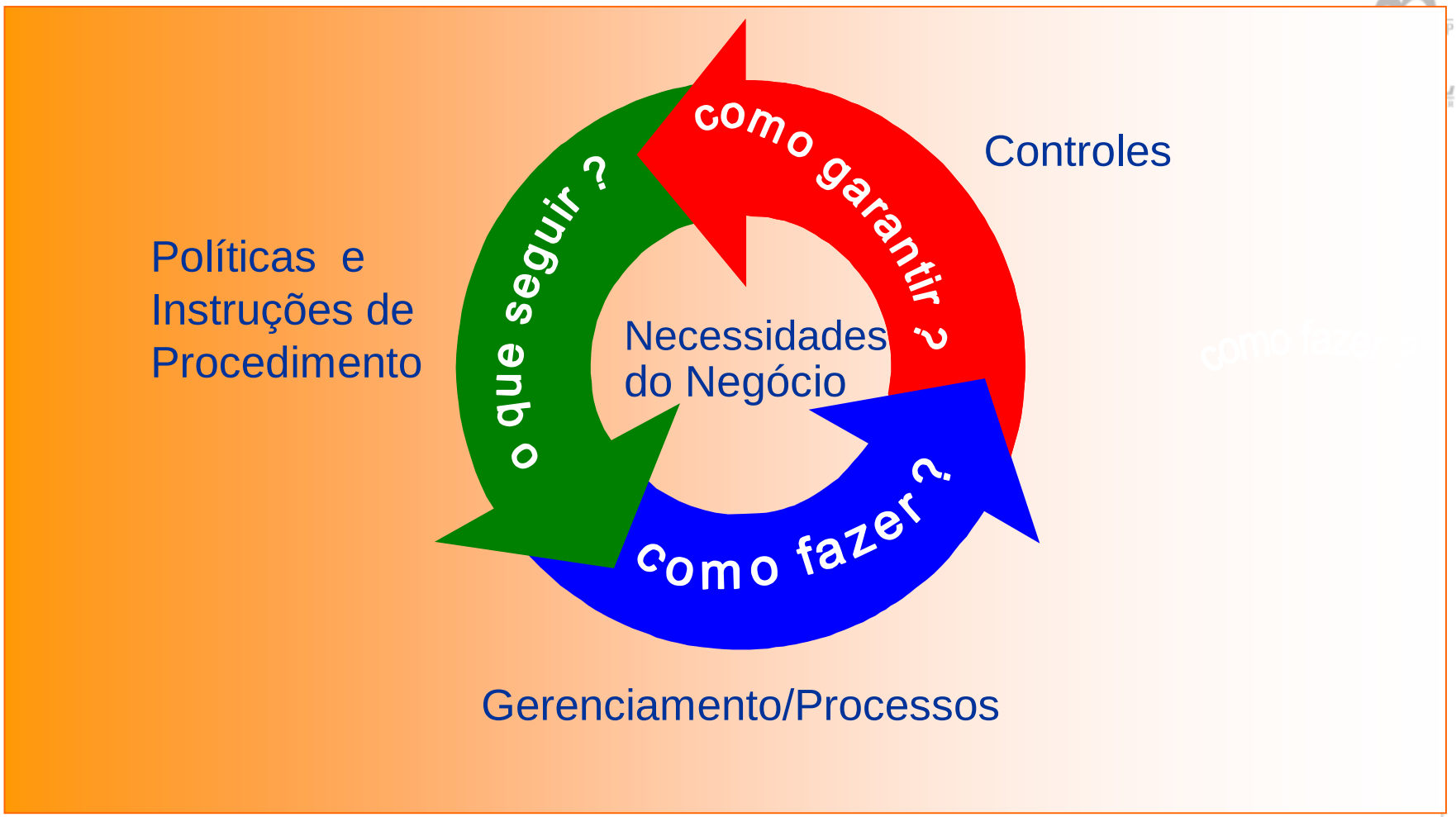
GESTÃO DE T.I.

José Luís Padovan
jlpadovan@gmail.com

Segurança da Informação

Estrutura de Segurança



Escopo da Gestão da Segurança

- Políticas
- Gerenciamento / Processos de Segurança
- Controles
- Pessoas

Políticas Corporativas Relevantes

- Corporativas
- RH
- Compras
- Jurídicas
- Compliance
- Financeiras

- Política de Privacidade
- Controle de Acesso
- Política Corporativa de Continuidade dos Negócios
- Política de Contratação de Consultoria
- Compra de Bens e Serviços não Produtivos
- Política Interna de Contratos
- Código de Conduta
- Gerenciamento de Risco e Conformidade Jurídica
- Política de Retenção de Registros Globais
- Política de Ativo
- Procedimento para a Proteção e Gerenciamento da Informação

Políticas de Segurança de TI

- Acesso
- Armazenamento
- Backup
- Escalonamento
- DRP
- Vírus
- Senhas

- Backup Corporativo
- Inclusão, Alteração e cancelamento de Acesso a Sistemas e Recursos de Informática
- DRP Processo de Acionamento
- Escalonamento de Incidentes de Segurança
- Acesso a Rede de Dados
- Prevenção e Detecção de Vírus
- Aprovação de Acesso a Sistemas Críticos de GMS e Financeiros
- Política de Uso de Senhas de Acesso à Rede
- Acesso a Internet

Políticas de Boas Práticas

Utilização de Recursos de TI

Atendimento

Instalação

Compras

- **Uso Adequado de Recursos de Tecnologia da Informação**
- **TI - Atendimento ao Negócio**
- **Utilização de Computadores e Periféricos, Notebooks e Handhelds**
- **Utilização de Ramais Telefônicos**
- **Sistemática de Utilização de Recursos de TI**
- **Utilização de Software**
- **Utilização de Telefones Celulares**
- **Utilização de Correio Eletrônico**
- **Utilização e Aquisição de Software**
- **Compra de Itens de TI**

Instruções de Procedimento

Acesso

Atendimento

Transferências

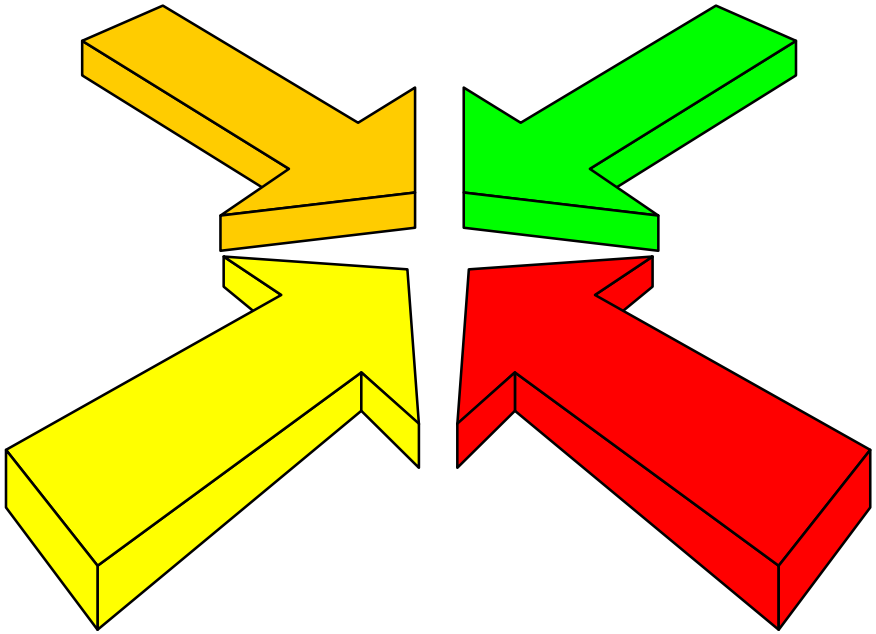
Gerenciamento de Mudanças

- Acesso a sala de Depósito de Material de TI
- Transferência de Equipamentos de TI
- Acesso a Sala de CPD
- Atendimento do SAN
- Desligamento de Funcionários de TI
- Funcionários de TI em Férias
- *Checklist* de validação do Perfil dos Usuários
- Procedimentos de segurança de "*History LOG Menus*"
- SAS - Sistema de Atualização de Software

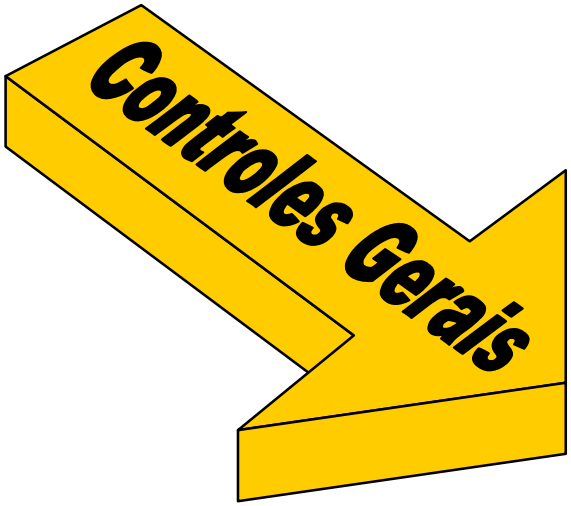
Gerenciamento / Processos de Segurança

- **Estabelecimento de indicadores e verificação periódica dos mesmos**
- **Estabelecimento de *checklists* de controle que deverão ser executados e registrados periodicamente com suporte de ferramentas de *workflow***
- **Estabelecimento de processos de comunicação tanto para o time de TI como para os usuários**
- **Estabelecimento de parcerias entre áreas como RH, Finanças e Jurídico**
- **Divulgação da política de segurança a novos colaboradores e reforço das ações através de eventos pontuais como a semana de TI**

Controles

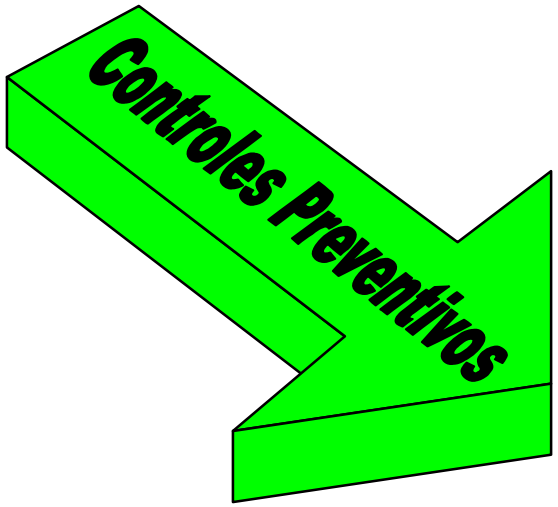


Controles



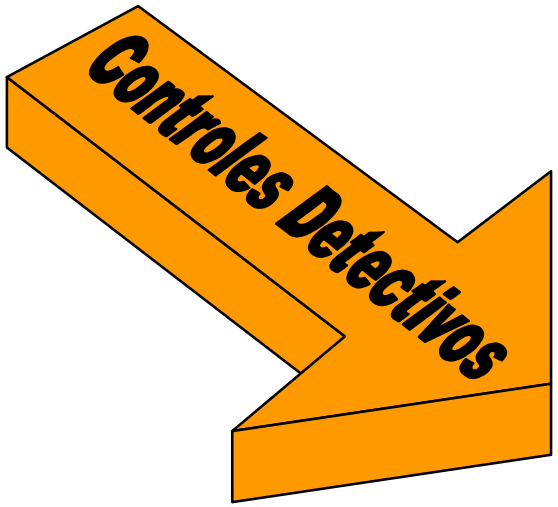
- Aplicabilidade e aderência das Políticas de Segurança
- Padrões de Hardware e Software
- Aplicabilidade das Metodologias
- Procedimentos de Atendimento aos usuários
- Procedimentos de Operação e Manutenção
- Políticas de Contratação e Demissão
- Atribuições e Responsabilidades
- Parceria com Controles Internos - Gerência de perfis de acesso a sistemas críticos
- Procedimentos para escalonamento de incidentes de segurança
- Duplo cheque para os principais controles implementados via ferramentas de *workflow* e sistema SMS

Controles



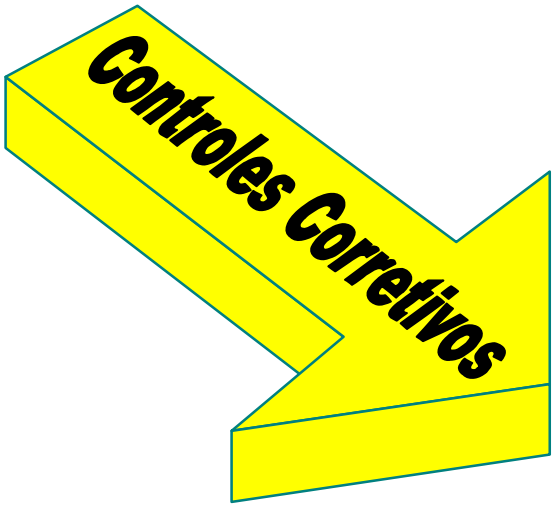
- Segregação de Funções / Ambientes
- Restrição de Acesso Físico / Lógico
- Controle de arquivos recebidos via e-mail
- Filtros anti-Spams
- Central de Controle de Vírus e distribuição de atualizações
- Firewall, Logins, IDS
- Classificação de Sites por conteúdo e bloqueio de categorias
- Bloqueio de download de certos arquivos via Internet
- Controle de publicação e verificação de integridade dos sites
- *Change Control*
- Scan de vulnerabilidade periódicos (internos/externos)
- Análise de vulnerabilidade de aplicações
- Inventário de software e controle de licenças
- Mecanismos de criptografia e autenticação forte para acesso remoto
- Controle do ambiente físico (câmeras, sensores de presença, sensores de umidade, controle de acesso a áreas restritas etc)
- Procedimentos de Backup e armazenamento de fitas em site externo
- Testes periódicos das fitas
- Risk Assessment periódicos
- Redundância de serviços críticos de telecom

Controles



- Análise de Mensagens de erro - alarme via SMS
- Análise diária e centralizada dos LOGs dos ativos de rede, de detecção, URLs visitadas e sistemas (Big Brother)
- Relatórios de Performance de Processamento
- Estabelecimento de Métricas e indicadores, e verificação periódica de seus resultados
- Scan de conteúdo nos servidores

Controles



- Planos de Continuidade de Negócio (BCP)
- Procedimentos de *Restore*
- Processo de *report* de incidentes de segurança
- Procedimentos automatizados para distribuição de software e patches

Pessoas - O elo mais Fraco

- Programa de Boas Vindas - Novos Funcionários
- Políticas com assinaturas de aceite e acesso via Intranet
- Guia de Boas Práticas para Utilização dos Recursos de TI
- Dia da Segurança - Semana de IT
- *Security Awareness*
- Assinatura de termos diversos para utilização de recursos
- Artigos na Dose Certa (Revista de circulação interna)
- *Pop-ups* de Segurança *da Intranet*
- Comunicados diversos
- SAN como ponto único de contato, para que os usuários falem com IT
- Treinamento de BCP

Gestão de T.I.

BCP

Business Continuity Plan

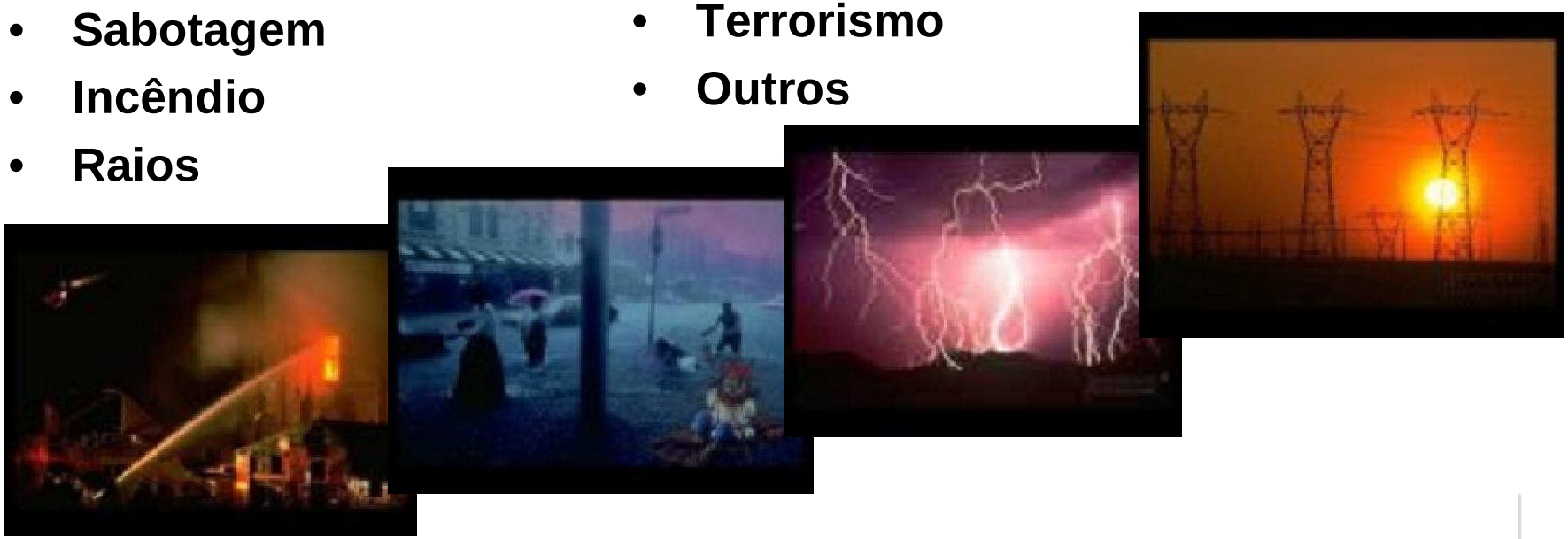
Fonte: Document Management – Maço/Abril 11

Sempre existe uma primeira vez !

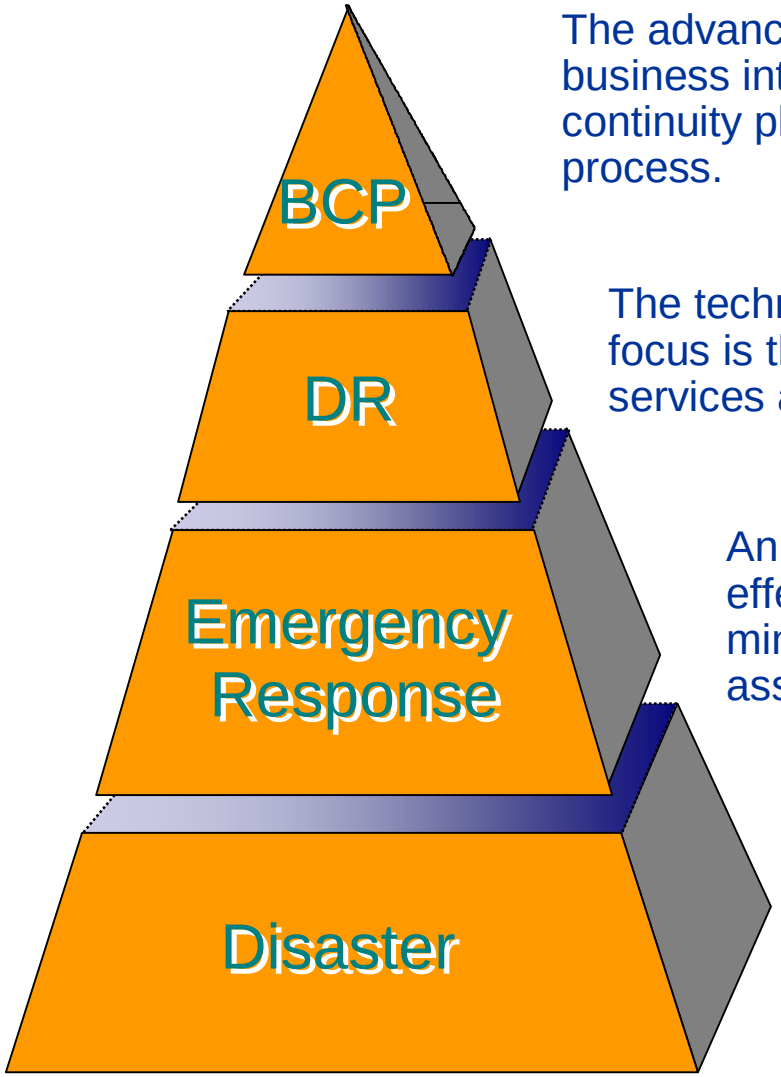
Tipos de Contingências (Desastres)

- Atos de Vandalismo
- Roubo
- Sabotagem
- Incêndio
- Raios

- Enchentes
- Acesso indevido
- Distúrbio civil
- Falha humana
- Explosão
- Terrorismo
- Outros



BCP and DRP in context



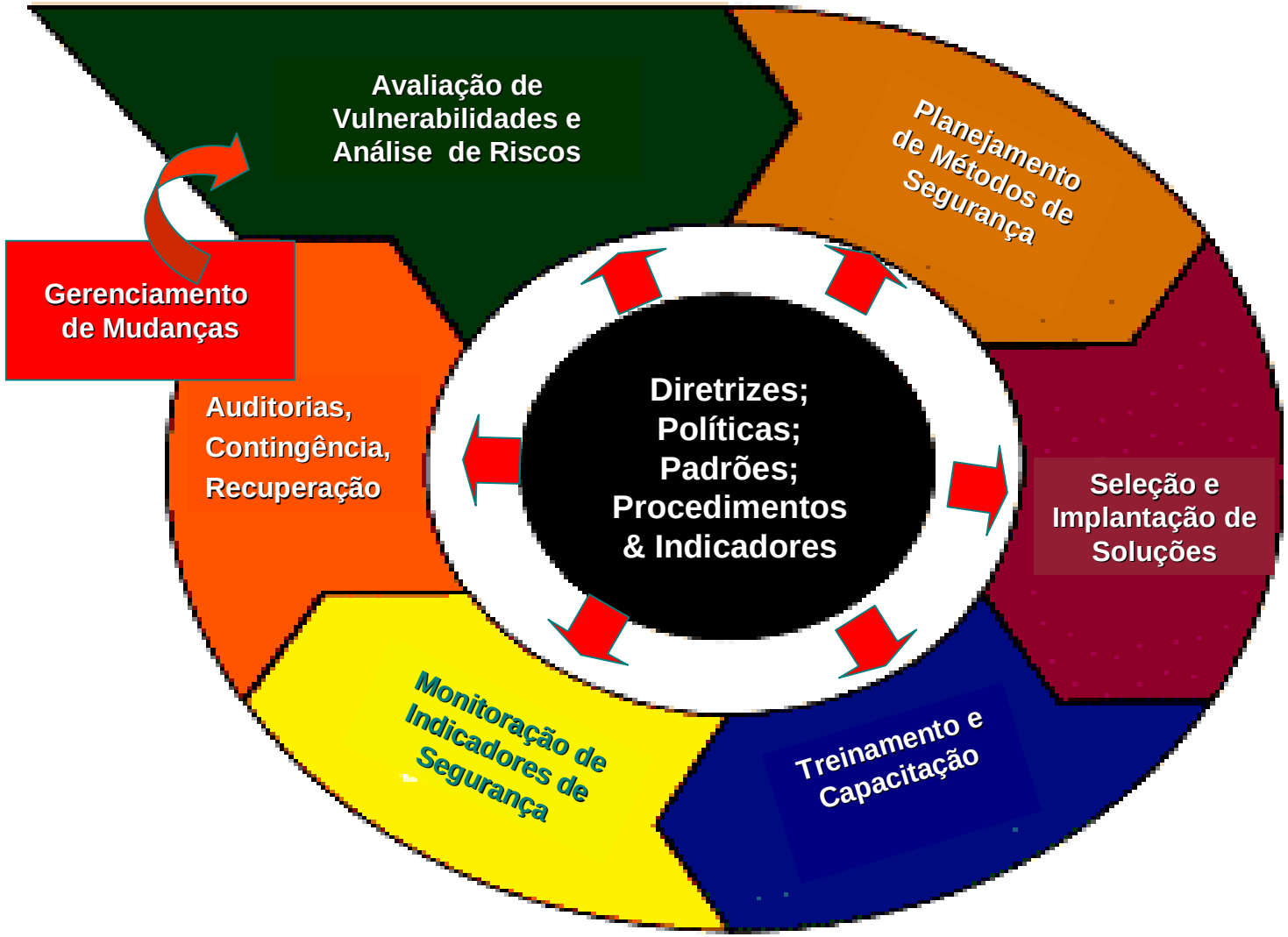
The advance preparations necessary to identify the impact of potential business interruptions; formulate recovery strategies; develop business continuity plans; and administer a training, exercise and maintenance process.

The technology aspects of a business continuity plan. Its focus is the restoration, at an alternate location, of data center services and computer processing capabilities.

An organization's coordinated response to a disaster in an effective and timely manner. The goal is to avoid or minimize injury to personnel and or damage to company assets.

An event, **anticipated or unanticipated**, that seriously disrupts normal business operations and prevents the company from delivering essential services for a period of time.

Metodologia



DEFINIÇÕES

- **Plano de Continuidade de Negócio**: “É o ato de antecipar incidentes, que podem afetar as funções e processos críticos de uma organização, assegurando-se de que responda a todo incidente de forma planejada”.

- **Disaster Recovery**: “É o processo de retorno ao estado normal das operações, ou a um nível mínimo aceitável de sobrevivênça interina”.

PORQUE DE UM PLANO DE CONTINUIDADE DE NEGÓCIO ?

- O planejamento eficaz da continuidade de negócio, poderá assegurar que todas as funções identificadas como sendo críticas dentro da organização estejam operacionais dentro dos tempos requeridos em caso de desastre.

OBJETIVOS DO BCP

- Minimizar o tempo de interrupção e os danos.
- Estabelecer meios alternativos das operações.
- Re-início das operações o mais cedo possível.
- Minimizar o impacto econômico.
- Minimizar o impacto de imagem.
- Assegurar que sejam observadas todas exigências legais.

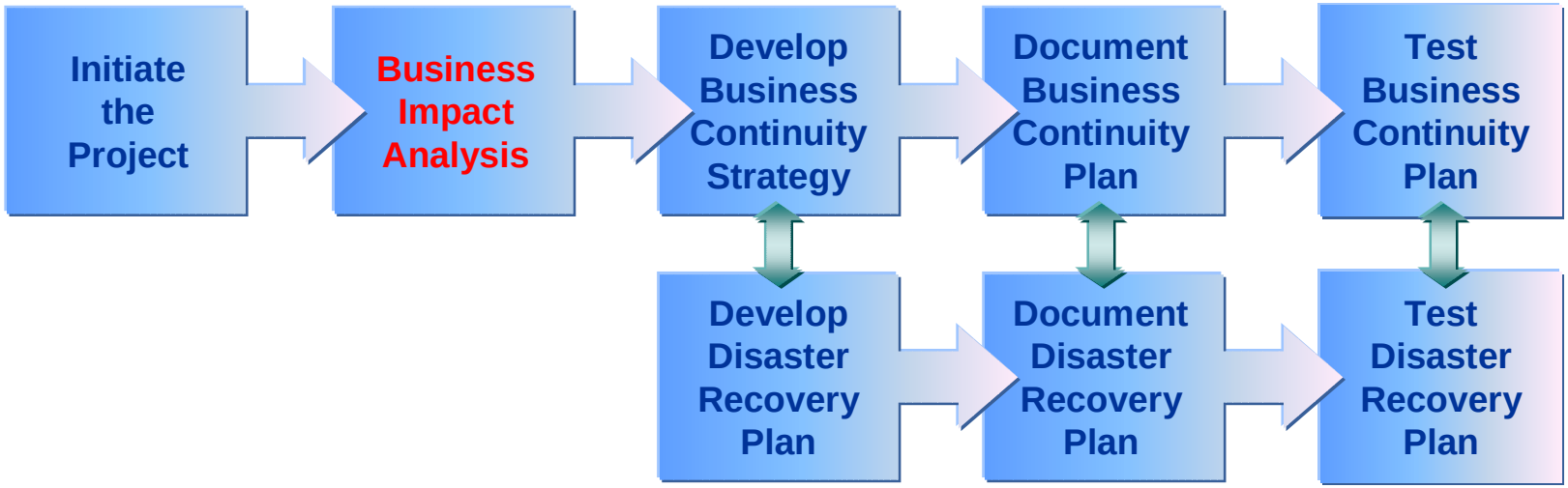
DO QUE É CONSTITUIDO UM BCP ?

- **Plano de Evacuação das Instalações**
- **Plano de Retorno a Normalidade das Operações**
- **Plano de Pernamência nas Instalações**
- **Plano de Acionamento do Ambiente de Trabalho de Contingência**
- **Plano de Recuperação do Ambiente de Trabalho**
- **Plano de Acionamento de Ambiente Tecnológico de Contingência**
- **Plano de Recuperação do Ambiente Tecnológico**

PLANEJAMENTO DOS PROCESSOS

- Início e Gestão do Projeto.
- Controle e Avaliação do Risco.
- Análise do impacto no Negócio.
- Segurança e Localização.
- Desenvolvimento de Estratégias de Recuperação.
- Resposta a Emergências.
- Desenvolvimento e Implementação de BCP (PCN).
- Procedimentos de Backup e Restore.
- Programa de Conscientização e Treinamento.
- Teste do Plano de Continuidade.
- Manutenção e Atualização do Plano de Continuidade.
- Estratégias de Salvamento e Recuperação.
- Auditoria e Revisão do Plano de Continuidade.

Business Continuity Planning Project Methodology



RISCO

Avaliação do Risco: É o processo de Identificação dos potenciais Riscos para Organização.

Análise de Impacto do Risco: É um processo desenvolvido e priorizado em um conjunto de recomendações para a redução do risco baseado no impacto que o risco poderá causar.

A avaliação e a análise do risco, irão identificar as áreas em que a organização poderá estar sob risco e onde, se os riscos não forem trabalhados, poderá resultar num desastre.

ÁREAS A AVALIAR

- Área a volta do Edifício.
- Estrutura do Edifício.
- Infra-estrutura Ambiental.
- Segurança Física.
- Controle de Acessos.
- Proteção ao Fogo.
- Armazenamento da Documentação.
- Segurança dos Dados Eletrônicos.
- Comunicações
- Monitoramento dos Alarmes.
- Energia Alternativa (UPS).

ANÁLISE DE IMPACTO NO NEGÓCIO

Uma análise do impacto no negócio, identifica os processos mais críticos e que se não forem recuperados a tempo após um desastre, trarão sérios impactos financeiros e de imagem para a organização.

- Nem todos os processos podem ser recuperados ao mesmo tempo.

- Custos em relação a necessidade.

  - ♦ Processos Obrigatórios,
  - ♦ Processos Necessários,
  - ♦ Processos Desejáveis.

INTERRUPÇÃO E RECUPERAÇÃO DAS ATIVIDADES

- Tempo máximo permitido.
- Tempo de recuperação dos sistemas computarizados.
- Tempo para ativação das instalações alternativas.
- Tempo de convocação dos colaboradores críticos
- Tempo para ativação dos equipamentos críticos.
- Impacto Financeiro.
- Interdependências funcionais e dos processos.

IMPACTOS

Impactos Financeiros Diretos.

- Perdas em Vendas.
- Atrasos nas Recepções.
- Pagamentos extras aos funcionários.
- Destruição de equipamentos e das facilidades.
- Custos com estadias para colaboradores
- Custos com locações de equipamentos e instalações
- Custos com serviços adicionais

IMPACTOS

Impactos Financeiros Indiretos.

- Exposições desfavoráveis na mídia.
- Perda da integridade dos dados.
- Perda de clientes ao longo do tempo.
- Impossibilidade no cumprimento de obrigações legais.
- Roubo ou Fraudes.
- Perda de confiança dos clientes, fornecedores, bancos e parceiros comerciais.

ESTRATÉGIA DE RECUPERAÇÃO

- A estratégia de recuperação é uma **indicação do nível elevado que mostra como uma organização** recuperará as suas diversas funções em situação de desastre.

- A estratégia de recuperação, **é o componente mais importante do plano de continuidade de negócio**, pois é nele onde são geridos todos os procedimentos de recuperação.

ÍNDICES DA ESTRATÉGIA

- O que será recuperado?
- Onde ocorrerá a recuperação?
- Como certos componentes devem ser recuperados?
- O que é requerido para a recuperação?
- Como acontecerá a recuperação?
- Como os sistemas funcionarão em ”Live”?

O PLANO

Deve ser:

- De uso simples,
- De fácil aprendizagem,
- De fácil manutenção,
- Projeto modular,
- De fácil adaptação.

REQUERIMENTOS PARA RECUPERAÇÃO

- Infraestruturas Alternativas.
- Equipamentos
- Redes Internas.
- Dados e Documentação.
- Equipamentos de Escritório.
- Estações de Trabalho.
- Equipes Treinadas (Colaboradores e Parceiros)
- Comunicações Externas

PROCESSO DE RECUPERAÇÃO

- Mobilização da equipe de gestão de emergências.
- Contato com a Mídia.
- Comunicação a Clientes, Fornecedores, Bancos e Parceiros Comerciais
- Mobilização da equipe de avaliação de danos
- Execução do BCP.
- Execução do DRP

FUNÇÕES DA EQUIPE DE GESTÃO DE EMERGÊNCIAS

- Elaborar e organizar o plano;
- Testar periodicamente o plano;
- Implementar Melhorias no plano;
- Promover o treinamento dos envolvidos com a execução do plano;
- Distribuir as novas versões do plano;
- Garantir a existência de cópias do plano fora do local;
- Controlar as cópias do plano;
- Implementar o Plano em Situação de Contingência

Business Continuity Planning Best Practices

- Obtain strong Executive sponsor
- Select two teams
  - Executive Team (Champions)
  - Operational Team (Doers)
- Make sure BCP is owned and driven by the organization, not IT
- Plan must support business goals and strategies
- Use methodology and tools
- Business Units own their risk
- Reporting and tracking of measurable deliverables
- Program flexibility
- Plan must be fully tested in production
- Establish BCP policies and procedures
- Build and institutionalize a BCP culture – be proactive instead of reactive
- Don’t skimp on the Business Impact Analysis, it is Critical!

Responsáveis por Segurança de TI

- Diretor de TI
- Gestores de Segurança - Security Officer
- Gestor de Infra-estrutura
- Gestor de Planejamento e Controle de TI

- **TODOS OS FUNCIONÁRIOS !!!**

Obrigado !