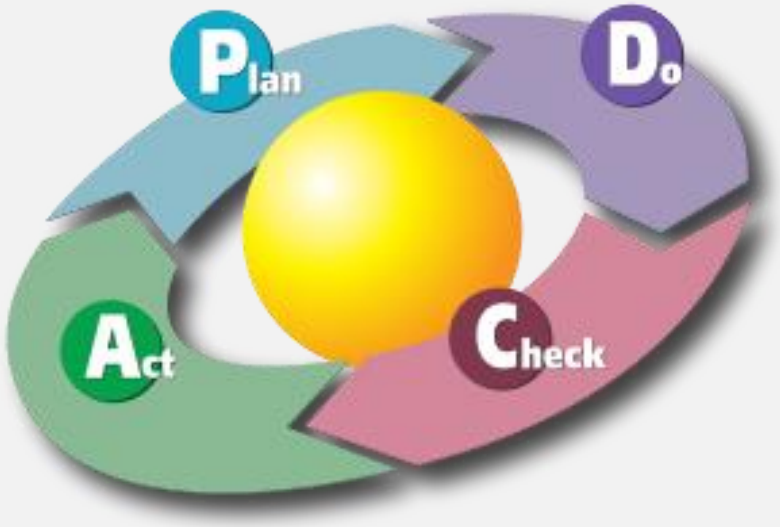
POLÍTICA DE SEGURANÇA E PLANO DE CONTINUIDADE

Prof. Me. Gabriel Caixeta Silva

PDCA



PLANEJAMENTO

- Baseada na ISO 27002.
- Identificação do requisitos de segurança:
  - Avaliação de risco.
  - Legislação e contratos.
  - Princípios, objetivos e requisitos de processamento.
  - POLÍTICA de SEGURANÇA da INFORMAÇÃO (**PSI**)

IMPLEMENTAÇÃO

- Colocar em prática o que foi planejado para atender aos requisitos da organização.
- Divulgação da PSI.
- Treinamento e conscientização dos usuários.
- Definição e documentação das normas, rotinas e procedimentos.
- Controles físicos e lógicos.

AVALIAÇÃO E AÇÃO CORRETIVA

- Verificar se a segurança implantada atende aos requisitos identificados na fase de planejamento.
- Análise crítica independente propõe que seja executada por auditoria interna, por um gestor independente ou por outra organização prestadora deste serviço.

NÍVEIS DE MATURIDADE

- Nível 1
  - Problemas de segurança tratados de forma pontual e baseada na iniciativa individual dos envolvidos.
  - Pouca ou nenhuma documentação.
  - Sem responsável formal.

NÍVEIS DE MATURIDADE

- Nível 2
  - Possui uma política.
  - Planos de contingência.
  - Procedimento de segurança documentados, mas são tratados a medida que são identificados.
  - Sem monitoração, avaliação de controles e correção de falhas.

NÍVEIS DE MATURIDADE

- Nível 3 - Proativo
  - Consistente e integrada.
  - Os ativos estão inventariados e classificados de acordo com seus requisitos de segurança.
  - Testes freqüentes.
  - Medidas corretivas.
  - Ambiente externos monitorado para identificação de novas ameaças.
  - Atualizações de segurança sistematicamente instaladas.

NÍVEIS DE MATURIDADE

- Nível 4 – Adição de valor
  - A segurança é vista como parte do negócio.
  - Tudo leva em conta princípios de segurança.
  - Alternativas de segurança são buscadas permanentemente.
  - Processos de gestão permitem antecipar problemas de segurança.

NÍVEIS DE MATURIDADE

- Ninguém é obrigado a estar no nível 4.
- Aceitável é pelo menos parte do nível 3.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- Documento que registra os princípios e as diretrizes de segurança adotados pela organização, a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos.

- Deve ser feita no mais alto nível da organização.

- Não deve ser estático, deve responder às mudanças. Revisões periódicas.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- **Organização da segurança**.
  - Estrutura organizacional.
- **Classificação e controle dos ativos de informação.**
  - Orientações sobre inventario e classificação de ativos.
- **Aspectos Humanos.**
  - Processos de admissão e demissão.
  - Comportamento de usuários.
- **Segurança ambiente físico.**
- **Segurança ambiente lógico.**
  - Operação correta e segura de recursos.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- **Segurança das comunicações.**
- **Prevenção e tratamento de incidentes**.
- **Desenvolvimento/aquisição, implantação e manutenção de sistemas**.
  - Todas as etapas do ciclo de vida de sistemas.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- **Gestão da continuidade.**
  - Recomendações para que a organização se prepare para neutralizar as interrupções.

- **Conformidade.**
  - Requisitos legais, normas e diretrizes internas e requisitos técnicos de segurança.
  - Procedimentos a serem adotados em caso de violação e direção das punições.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- Divulgação.
  - Quase tão importante quanto a própria PSI.
  - Pode-se destacar trechos .
    - Grupo de faxineiros.
    - Grupo de porteiros
    - Aproveitar-se de algum evento recente.

ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

- Estrutura organizacional.
  - Conjunto de responsabilidades, autoridades relações entre pessoas de uma organização.
- Cada organização pode ter a sua estrutura, baseada no tamanho, grau de maturidade, etc.
- Organizações pequenas: endossar a PSI.
- Maiores: comitê de segurança.
- Em todos os casos um gestor de segurança deve ser designado.

PLANO DE CONTINUIDADE DE NEGÓCIOS PCN

INTRODUÇÃO

Refere-se a um conjunto de **estratégias** e **planos** de **ação preventivos** que **garantem** o pleno **funcionamento** dos **serviços essenciais** de uma empresa durante quaisquer tipos de falhas, até que a situação seja normalizada.

Tem a finalidade de criar **normas e padrões** para que, em **situações adversas**, as empresas possam **recuperar**, **retomar** e **dar** prosseguimento aos seus mais cruciais processos de negócio, evitando que eles sofram danos mais profundos que provoquem perdas financeiras.

CONDIÇÕES ESSENCIAIS PARA ELABORAÇÃO

Análise de risco: o que de ruim pode vir a acontecer? (principais ameaças)

Análise de impacto: de que forma eventuais ameaças podem impactar o negócio?

Planejamento estratégico: se uma ameaça se apresentar, quais atitudes e ações se fariam necessárias para a retomada das operações?

ESTRUTURA DE UM PCN

Plano de Contingência (Emergência): deve ser utilizado em último caso, quando todas as prevenções tiverem falhado. Define as necessidades e ações mais imediatas.

Plano de Administração ou Gerenciamento de Crises (PAC): define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência.

ESTRUTURA DE UM PCN

Plano de Recuperação de Desastres (PRD): determina o planejamento para que, uma vez controlada a contingência e passada a crise, a empresa retome seus níveis originais de operação.

Plano de Continuidade Operacional (PCO): seu objetivo é restabelecer o funcionamento dos principais ativos que suportam as operações de uma empresa, reduzindo o tempo de queda e os impactos provocados por um eventual incidente. Um exemplo simples é a queda de conexão à internet.

CLASSIFICAÇÃO DE ATIVOS

PRA VARIAR ...

- Não existe uma forma padronizada de se classificar a informação existente nas organizações.
- Conforme ISO 27002.
  - Contabilização dos ativos.
  - Classificação da informação.

CONTABILIZAÇÃO DOS ATIVOS

- Tem como exemplos:
  - Bases se dados e arquivos.
  - Documentação de sistemas.
  - Manuais de usuário.
  - Material de treinamento.
  - Procedimentos de suporte ou operação.
  - Planos de continuidade.
  - Procedimentos de recuperação.
  - Informações armazenadas.

CONTABILIZAÇÃO DOS ATIVOS

- Software:
  - Aplicativos
  - Sistemas
  - Ferramentas de desenvolvimento.
- Ativo físicos:
  - Processadores.
  - Modems
  - Roteadores.
  - Moveis

CONTABILIZAÇÃO DOS ATIVOS

- Serviço:
  - Comunicação.
  - Aquecimento.
  - Iluminação.
  - Refrigeração.
- Deve ter o registro de sua localização.
- É essencial para uma gestão patrimonial e boa administração dos riscos de segurança.

CLASSIFICAÇÃO DOS ATIVOS

- Se todas as informações são importantes, temos que proteger tudo.

CONTABILIZAÇÃO DOS ATIVOS

- Uma coisa pode impactar em outra.
  - Confidencialidade x Disponibilidade

A classificação deve ser revista de tempos em tempos.

Ex: Lançamento de um produto.

REQUISITOS DE CONFIDENCIALIDADE

Tipo	Características	Exemplo
Confidencial	A divulgação para pessoas não autorizadas pode causar danos graves à organização.	Numa operadora de telefonia, as informações pessoais e sobre cobrança dos clientes, se indevidamente reveladas, podem levar, por exemplo, a penalidades legais por invasão de privacidade ou a prejuízos financeiros causados pela exploração dos dados por um concorrente disposto a capturar os clientes mais lucrativos da empresa por meio de ofertas mais vantajosas.
Reservada	Informações que no interesse da organização devam ser de conhecimento restrito e cuja revelação não autorizada pode frustrar o alcance de objetivos e metas.	Detalhes do lançamento de um novo produto podem atrapalhar os planos de uma empresa caso cheguem ao conhecimento da concorrência antes do momento oportuno.
Pública	Informação de livre acesso.	Informações institucionais publicadas no *site* da organização.

REQUISITOS DE DISPONIBILIDADE

Tipo	Características	Exemplo
Exigência de recuperação em curto espaço de tempo (pode abranger as categorias 1 e 2)	A indisponibilidade além de um breve período de tempo pode causar prejuízos inaceitáveis.	Sistemas que viabilizam a realização de transações em instituições financeiras que atuam no mercado de ações.
Exigência de recuperação em médio espaço de tempo (pode abranger as categorias 2, 3 e 4)	A indisponibilidade temporária não compromete o desempenho dos processos críticos, mas após determinado período pode causar atrasos ou decisões equivocadas que se deseja evitar.	Informações de apoio às atividades gerenciais rotineiras, tais como resultados de vendas, indicadores de produção etc.

REQUISITOS DE DISPONIBILIDADE

Sem exigência de tempo de recuperação (categoria 6)	A perda ou indisponibilidade por longo período não traz impactos negativos consideráveis, seja pela facilidade de recuperação da informação em fontes externas ou internas, seja por sua pouca relevância para os processos organizacionais.	Informações sobre os horários de vôo para os destinos mais comuns das viagens de funcionários disponíveis numa Intranet (a informação é útil para agilizar a marcação de compromissos de trabalho, mas pode ser facilmente recuperada em *sites* de agências de viagem ou companhias aéreas).
Exigência de tempo de recuperação sujeita a sazonalidade (categoria 5)	O tempo aceitável de indisponibilidade é variável.	Sistema que roda a folha de pagamento ou que gera automaticamente a cada mês os pedidos de compra para produtos em falta no estoque.

REQUISITOS DE INTEGRIDADE

Tipo	Características	Exemplo
Alta exigência de integridade	A criação com erro ou alteração indevida pode comprometer as operações ou os objetivos organizacionais, acarretar descumprimento de normas legais ou trazer prejuízos à organização, a seus integrantes ou à sociedade.	No governo, informações que dão origem à concessão de benefícios pela Previdência Social (a fragilidade dos mecanismos de proteção da integridade dos dados pode levar à ocorrência de fraudes e ao pagamento indevido de benefícios). Numa operadora de telefonia, a falta de integridade dos dados de cobrança dos clientes pode causar problemas graves (além da insatisfação dos clientes, penalizações pelo não-cumprimento das metas previstas pela Anatel em relação ao limite de reclamações permitidas a cada mil contas). Numa fábrica, um pedido registrado incorretamente pode levar a prejuízos causados por descumprimento de cláusulas contratuais ou pelo desencadeamento de processos custosos de produção que não deveriam ter sido acionados.

REQUISITOS DE INTEGRIDADE

Média exigência de integridade	A criação com erro ou alteração indevida não compromete as operações nem traz impactos exagerados, mas pode causar algum prejuízo.	Preço de mercadorias vendidas a ser publicado num anúncio (um erro no preço pode implicar a venda da quantidade anunciada do produto com prejuízo).
Baixa exigência de integridade	A criação com erro ou alteração indevida pode ser facilmente detectada e/ou oferece riscos desprezíveis para a organização.	Preços de insumos coletados dos fornecedores (um erro no preço registrado será facilmente descoberto durante o processo de negociação e compra).

REQUISITOS DE AUTENTICIDADE

Tipo	Características	Exemplo
Com exigência de verificação de autenticidade	Informação cuja procedência precisa ser confirmada antes de sua utilização.	Pedido de criação de senha de acesso para um usuário de sistema, comunicados públicos em nome da organização, informações relativas a transações financeiras, sistemas de publicação eletrônica disponíveis para o público.
Sem exigência de verificação de autenticidade	Informação cuja procedência não precisa ser confirmada antes do seu uso ou divulgação.	