7.0 - Gerenciamento de Riscos e Plano de Continuidade de Negócios

prof. Fábio Engel

fabioe@utfpr.edu.br

Conteúdo

1. Definição de Gerenciamento de Riscos
2. Identificação de riscos
3. Análise de Risco
   - Análise qualitativa de riscos
   - Análise quantitativa de riscos
4. Planejamento de respostas a riscos
5. Monitoramento e controle de riscos
6. Implementação de uma BIA, um BCP e um DRP
   - Análise de impacto nos negócios
   - Plano de continuidade de negócios
   - Plano de recuperação de desastre

Definição de Gerenciamento de Riscos

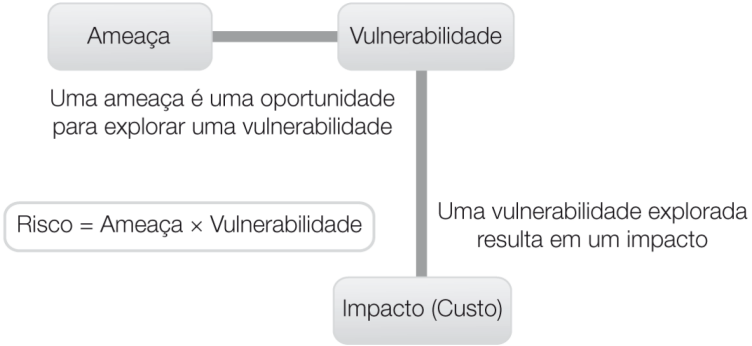
- **Risco** é a probabilidade de que um evento incerto afete um ou mais recursos.
- **Gerenciamento de riscos** é o processo de identificar, avaliar, priorizar e enfrentar riscos. Qualquer organização séria a respeito de segurança verá essa questão como um processo contínuo.
- Gerenciamento de riscos garante que você tenha planejado riscos mais prováveis de terem um efeito sobre sua organização. Uma organização segura tem planos estabelecidos para enfrentar riscos antes que eventos ocorram.

Definição de Gerenciamento de Riscos

- O corpo de conhecimento de gerenciamento de projeto (PMBOK - *Project Management Body of Knowledge*) mantido pelo Instituto de Gerenciamento de Projeto (PMI - *Project Management Institute*) estabelece que os efeitos de riscos podem ser positivos ou negativos.
- O PMI baseia sua filosofia de gerenciamento de riscos em uma abordagem proativa, que, simultaneamente:
  - Minimiza os efeitos de riscos negativos.
  - Maximiza os efeitos de riscos positivos.

Definição de Gerenciamento de Riscos

- A figura abaixo mostra o relacionamento clássico entre riscos, ameaças e vulnerabilidades.



Definição de Gerenciamento de Riscos

- Muitas pessoas nunca pensaram em risco como algo positivo. Porém, a incerteza pode resultar em eventos que possuam efeitos negativos ou positivos.
  - Por exemplo, suponha que sua organização planeje distribuir um novo software para seus usuários com base em disponibilidade projetada a partir de seu vendedor de software. Seu plano de gerenciamento de riscos deverá considerar as respostas tanto para uma entrega adiantada de software como para uma atrasada.
    - Se receber adiantadamente o software, você poderá realizar um teste mais completo ou iniciar a distribuição mais cedo.
    - Se seu vendedor de software atrasar na entrega do produto, você poderá perder a data de distribuição projetada.
    - Você deverá ter planos estabelecidos para enfrentar tanto os efeitos positivos como os negativos de uma data de entrega que não corresponda ao cronograma.

Definição de Gerenciamento de Riscos

- Uma **metodologia de riscos** é uma descrição de como você gerenciará riscos.
- A metodologia de risco que sua organização adotar deverá incluir a abordagem, a informação exigida e as técnicas para enfrentar cada risco.
- A abordagem define como você executará as etapas do processo de metodologia de riscos.

Definição de Gerenciamento de Riscos

- O processo de gerenciar riscos começa por identificá-los. De acordo com o PMI, as etapas são:
    1. Identificação de riscos.
    2. Análise de riscos.
    3. Planejamento de resposta a riscos.
    4. Monitoramento e controle de riscos.

Identificação de riscos

- **1. Identificação de riscos**
  - É o processo de determinar e classificar os riscos que podem afetar seus recursos.
    - A capacidade de identificar riscos é uma parte fundamental de um processo efetivo de gerenciamento de riscos.
    - Essa identificação deverá envolver o máximo possível de pessoas trabalhando em diferentes funções. Ter mais pessoas envolvidas permite que você identifique riscos a partir de vários pontos de vista.

Identificação de riscos

- O resultado do processo de identificação de riscos é uma lista de riscos identificados. O PMI a chama de **registrador de riscos**, que pode conter muitos tipos diferentes de informação, mas deve conter pelo menos:
  - Uma descrição do risco.
  - O impacto esperado se o evento associado ocorrer.
  - A probabilidade de o evento ocorrer.
  - Medidas para atenuar o risco.
  - Medidas a serem tomadas se o evento ocorrer.
  - Classificação do risco.

Identificação de riscos

- Você pode preencher apenas parte do registrador de riscos durante esta fase. O objetivo é documentar o máximo de riscos possível.
- Você poderá coletar entradas para o registrador de riscos de várias maneiras, incluindo:
  - Reuniões de *brainstorming* para identificação de riscos.
  - Pesquisas formais.
  - Consultas informais e solicitações de comentário.
  - Eventos de incentivo, como "intervalos para um café e troca de idéias", que incluam um fórum para colher comentários e retornos.

Identificação de riscos

- **Análise de Risco**
  - A próxima etapa é analisar os riscos identificados para decidir como classificá-los.
  - Toda organização possui orçamento limitado, não podendo responder a cada risco em potencial.
  - A análise de risco permite que as organizações decidam quais riscos exigem mais atenção.
  - As organizações usam duas técnicas comuns para analisar riscos:
    - Análise qualitativa de riscos.
    - Análise quantitativa de riscos.

Análise qualitativa de riscos

- Análise qualitativa de riscos
  - **Análise qualitativa de riscos** utiliza classificação relativa para determinar respostas a riscos.
  - Usa probabilidade e impacto de riscos.
  - Você geralmente expressará probabilidade de risco como relativa, da seguinte forma:
    - **Alta probabilidade** - Muito provável de ocorrer.
    - **Média probabilidade** - Nem frequente nem rara.
    - **Baixa probabilidade** - Não muito provável de ocorrer.
  - Outra forma seria através do impacto que causam, podendo varia de baixo (desprezível) a alto (substancial).

Análise qualitativa de riscos

- Diferentes organizações podem escolher diferentes classificações para probabilidade e impacto de riscos.
- A análise qualitativa rapidamente prioriza riscos para realizar análises adicionais e planejamento de respostas a eles.

Análise quantitativa de riscos

- Análise quantitativa de riscos
  - **Análise quantitativa de riscos** utiliza fórmulas matemáticas e números para classificar sua severidade. Seu objetivo é quantificar possíveis resultados de riscos, determinar probabilidades de resultados, identificar riscos de alto impacto e desenvolver planos com base em riscos
    - Você pode usar análise quantitativa de riscos para todo risco no registrador, mas a quantidade de esforço exigida pode ser demasiada para riscos de baixa probabilidade ou baixo impacto. Por esse motivo, a análise quantitativa de riscos geralmente começa com aqueles considerados de alta probabilidade durante a análise qualitativa.

Análise quantitativa de riscos

- Aqui estão as etapas envolvidas na realização de uma análise quantitativa de riscos para cada item em seu registrador:
    1. Calcule a exposição ao risco.
        a. Atribua um valor a cada recurso.
        b. Determine a porcentagem de perda para cada ameaça realizada. Esse valor é o **fator de exposição** (**EF** - *Exposure Factor*) para a ameaça contra um recurso.
    2. Calcule a perda para uma única ocorrência de ameaça, chamada **expectativa de perda única** (**SLE** - *Single Loss Expectancy*), usando a seguinte fórmula:
        - SLE = valor de recurso $\times$ EF

Análise quantitativa de riscos

- Aqui estão as etapas envolvidas na realização de uma análise quantitativa de riscos para cada item em seu registrador:
    3. Calcule ou determine a probabilidade anual de uma perda. A probabilidade anual estimada de que uma ameaça indicada será realizada é chamada de **taxa de ocorrência anual (ARO - Annual Rate of Occurrence)**.
    4. Calcule a perda anual estimada devido a uma ameaça realizada específica, chamada **expectativa de perda anual (ALE - Annual Loss Expectancy)**, usando a seguinte fórmula:
        - $\text{ALE} = \text{SLE} \times \text{ARO}$

Análise quantitativa de riscos

- A tabela abaixo contém alguns riscos como exemplos e a ALE calculada para cada risco. Uma vez que tenha uma ALE para cada risco, você poderá determinar quais riscos enfrentar primeiro.

TABELA 4.1 Análise quantitativa de riscos

RECURSO	RISCO	VALOR	EF	SLE	ARO	ALE
Prédio	Incêndio	$700.000	0,60	$420.000	0,20	$ 84.000
Servidor de arquivos	Falha de disco	$ 50.000	0,50	$ 25.000	0,20	$ 5.000
Dados confidenciais	Roubo	$200.000	0,90	$180.000	0,70	$126.000
Conexão de negócio eletrônico com a Internet	Indisponibilidade por uma hora	$ 15.000	1,00	$ 15.000	12,00	$180.000

Planejamento de respostas a riscos

- **3. Planejamento de respostas a riscos**
  - Depois de identificar e classificar o máximo de riscos possível, a próxima etapa é selecionar estratégias para enfrentar cada um. Você deverá inclui-las no registrador de riscos.
  - Seu plano de resposta a risco mostra que você os examinou e desenvolveu planos para enfrentá-los. É importante que você inclua uma descrição de resposta para cada risco no registrador.
  - Para cada resposta a um risco, você deverá atribuir um ou mais "proprietários" para executar as ações planejadas.

Planejamento de respostas a riscos

- Existem quatro respostas para **riscos negativos**:
    1. **Evitar** - Ameaça é eliminada mudando recursos ou a infraestrutura de TI. Por exemplo, adição de links redundantes.
    2. **Transferir** - O risco é deslocado para um terceiro. Por exemplo, comprar seguro contra incêndio desloca o risco associado para a companhia que mantém a apólice.
    3. **Atenuar** - Redução da probabilidade ou o impacto do risco. Por exemplo, para atenuar ataques conhecidos, você pode reforçar servidores web atualizando software e alterando opções de configuração.
    4. **Aceitar** - Nenhuma medida é tomada em resposta. Você pode aceitar um risco se os efeitos não compensarem a despesa de uma resposta.

Planejamento de respostas a riscos

- Para riscos positivos, as resposta incluem:
    1. **Explorar** - Tira proveito de uma oportunidade que surge quando responde a esse risco. Por exemplo, suponha que sua organização tenha desenvolvido materiais de treinamento para uso interno para ajudá-lo a enfrentar um risco específico. Esse material poderia ser embalado e comercializado.
    2. **Compartilhar** - Utiliza-se um terceiro para ajudar a capturar a oportunidade associada a esse risco. Por exemplo, comprar um grupo de licenças de estações de trabalho junto com outra organização permite que ambas as organizações ganhem um desconto devido ao tamanho do pedido combinado.

Planejamento de respostas a riscos

- Para riscos positivos, as resposta incluem:
    3. **Aprimorar** - Aumenta a probabilidade ou o impacto positivo do evento associado ao risco. Por exemplo, suponha que você tenha um contrato para entregar software, que inclua um bônus pará término adiantado. Para aprimorar o risco, você poderia oferecer a uma empresa subcontratada um bônus (menor que o ganho) para terminar antes do prazo.
    4. **Aceitar** - Não toma-se medidas para enfrentá-lo, pois seus efeitos em potencial são positivos e agregam valor.

- **4. Monitoramento e controle de riscos**
  - Você não deverá realizar identificação e análise de risco apenas uma vez.
  - As condições de uma organização mudam constantemente, assim como os riscos encontrados por ela.
  - É preciso monitorar riscos continuamente e realizar uma análise adicional para desenvolver novas respostas a riscos sempre que identificar novos.
  - O processo formal de monitorar e controlar riscos foca a identificação e análise de novos riscos e o rastreamento daqueles identificados anteriormente.

Monitoramento e controle de riscos

- Os riscos deverão ser reavaliados quando ocorrer qualquer um dos seguintes eventos:
  - Identificação de evidência de que uma ameaça foi observada ou está em vias de ser.
  - Aprovação, pela empresa, de uma solicitação de mudança em seu plano de resposta a riscos.
  - Ocorrência de mudança em seu ambiente que possa afetar riscos de recursos.
  - Aplicação de ações corretivas ou preventivas.

- **Implementação de uma BIA, um BCP e um DRP**
  - O foco principal de gerenciamento de riscos é antecipar-se a ameaças observadas.
  - Não é possível prever e impedir **cada** evento que resulte em perda. Isso significa que ainda existe a probabilidade de que qualquer organização encontre um evento que interromperá as operações normais dos negócios.
  - Segurança de informação exige que qualquer informação esteja disponível quando qualquer usuário autorizado precisar dela. Você terá de desenvolver e implementar métodos e técnicas para proteger os recursos de TI da organização e garantir que eventos não interrompam as funções normais de negócios.

Análise de impacto nos negócios

- O primeiro passo ao desenvolver planos para enfrentar interrupções é identificar as funções de negócios cruciais para sua organização.
- Quando um evento interrompe a capacidade de sua organização realizar operações, é importante restaurar as mais cruciais primeiro. Antes disso, você terá de identificar quais são essas funções.

Análise de impacto nos negócios

- Uma **análise de impacto de negócios** (BIA - *Business Impact Analysis*) é uma análise formal das funções e atividades de uma organização, que as classifica com críticas ou não.
  - Funções críticas são exigidas para executar os negócios. Se não executadas, seu dano será inaceitável. Funções não críticas podem ser importantes, porém não impedem uma organização de realizar negócios.
  - Uma BIA também organiza as atividades críticas com base em importância e ajuda uma organização a determinar quais funções restaurar e em que ordem, no caso de uma interrupção importante.

Análise de impacto nos negócios

- Na BIA, a seção para cada função crítica recebe informações adicionais, incluindo uma descrição de objetivos e requisitos de recuperação para cada uma.
- Objetivos e requisitos são expressos da seguinte maneiras:
    a) **Objetivo de ponto de recuperação (RPO - Recovery Point Objective)** - A quantidade de perda de dados aceitável. Dependendo da natureza da função, membros da equipe podem ser capazes de recriar ou reinformar dados. O RPO orienta se prevenção ou correção de perda é melhor opção.

Análise de impacto nos negócios

- b) **Objetivo de tempo de recuperação (RTO - Recovery Time Objective)** - O tempo máximo permitido para recuperar a função. Muitos planos de recuperação menos formais desconsideram RTO. O tempo pode ser um fator crítico, e especificar os requisitos para tempo de recuperação ajudará a determinar as melhores opções.
- c) **Requisitos de recuperação de negócios** - Qualquer pré-requisito de negócios para as funções - ou seja, outras funções de negócios que já precisarão estar prontas para que as funções de recuperação ocorram. Requisitos de recuperação de negócios ajudam a determinar a sequência de recuperação.
- d) **Requisitos de recuperação técnica** - Qualquer pré-requisito técnico para dar suporte a cada função de negócios. Na maioria dos casos, requisitos de recuperação técnica determinam quais componentes de infraestrutura de TI precisarão estar preparados.

Análise de impacto nos negócios

- A BIA ajudará a identificar não apenas quais funções são críticas, mas também com que rapidez as funções essenciais de negócios precisarão retornar à plena operação após uma interrupção importante.
- A BIA também identificará requisitos de recursos para retornar cada função à operação plena.
- Uma BIA sólida indicará os requisitos necessários para conduzir negócios por um período estendido quando a infraestrutura normal estiver indisponível.

Plano de continuidade de negócios

- Um **plano de continuidade de negócios** (BCP - *Business Continuity Plan*) é um plano para uma resposta estruturada a qualquer evento que resulte em uma interrupção de atividades ou funções críticas de uma empresa.
- Realizar uma BIA é um primeiro passo importante para gerar BCP, no sentido de que a BIA identifica os recursos para os quais um BCP é necessário.

Plano de continuidade de negócios

- BCP trata principalmente dos processos, recursos, equipamentos e dispositivos necessários para continuar a condução de atividades críticas de uma empresa no caso de uma interrupção que afete a viabilidade dos negócios.
- A parte mais importante é definir prioridades, com o entendimento de que pessoas sempre vêm em primeiro lugar.

Plano de continuidade de negócios

- A ordem de prioridades para um BCP bem balanceado deverá ser a seguinte:
  1. Segurança e bem-estar de todas as pessoas.
  2. Prédios e instalações.
  3. Componentes de infraestrutura, incluindo comunicações e sistemas de informação.

Plano de continuidade de negócios

- Um BCP formal não é apenas útil para muitas organizações - em algumas circunstâncias, é obrigatório. Legislação e regulamentações normalmente exigem um BCP para garantir que sistemas estejam seguros.
- O custo de tempo de paralisação de sistemas para essas empresas pode ser extremo. Custos diretos e indiretos associados ao tempo de paralisação podem existir em diversas categorias, inclusive:
  - Clientes perdidos
  - Receita perdida
  - Fatia de mercado perdida
  - Despesa adicionais
  - Reputação prejudicada

Plano de continuidade de negócios

- Organizações precisam considerar planos de contingência e recuperação a partir de um ponto de vista abrangente.
- Manter o contexto mais amplo em vista, durante o desenvolvimento do plano, permitirá enfrentar os riscos de uma organização, ao contrário de apenas consertar um recurso arruinado.
- Os elementos de um BCP completo deverão incluir:
  - Resposta a emergências e proteção de vida e segurança.
  - Avaliação de situação e de danos.
  - Salvamento e recuperação de recursos.
  - Instalações alternativas para operação de emergência e recuperação de negócios.

Plano de continuidade de negócios

- Resumindo, um BCP direciona todas as atividades exigidas para garantir que as funções críticas de negócios de uma organização continuem com pouca ou nenhuma interrupção.
- O BCP supõe que os **componentes de infraestrutura necessários para dar suporte a operações estejam em vigor**. Infelizmente, isso nem sempre é o caso após um desastre.
  - O que acontecerá de um incêndio destruir seu centro de dados?
  - A resposta é outro plano, um plano de recuperação de desastre.

Plano de recuperação de desastre

- Um **Plano de recuperação de desastre** (DRP - *Disaster Recovery Plan*) direciona as ações necessárias para recuperar recursos após um desastre.
- Um DRP faz parte de um BCP e é necessário para garantir a restauração de recursos exigidos pelo BCP até um estado disponível.
- O DRP estende e dá suporte ao BCP, identificando eventos que possam causar danos a recursos necessários para dar suporte a funções críticas de negócios.

Plano de recuperação de desastre

- O BCP já contém uma lista dos recursos necessários para dar suporte a cada função de negócios.
- O próximo passo ao desenvolver um DRP é considerar o que poderia acontecer a cada recurso.

Plano de recuperação de desastre

- Análise de Ameaça
  - Uma análise de ameaça envolve identificar e documentar ameaças a recursos críticos.
  - Antes que possa se recuperar de um desastre, é preciso considerar quais tipos de desastres são possíveis e quais tipos de danos podem causar.
  - Algumas ameaças incluem:
    - Incêndio
    - Inundação
    - Furação
    - Tornado
    - Doença
    - Terremoto
    - Ciberataque
    - Sabotagem
    - Terrorismo

Plano de recuperação de desastre

BCP e DRP: Qual é a diferença?

Um BCP não especifica como se recuperar de desastres, apenas de interrupções. Em geral, uma interrupção é um evento menor que pode atrapalhar um ou mais processos de negócios por um curto período. Ao contrário, um desastre é um evento que afeta vários processos de negócios por um período estendido. Desastres normalmente também causam danos substanciais a recursos que você precisará tratar antes que possa resolver a interrupção do processo de negócios.

Plano de recuperação de desastre

- Cenários de impacto
  - Após definir ameaças em potencial, o próximo passo ao criar um DRP abrangente é documentar cenários prováveis de impacto, a base do DRP.
- Documentação de Requisito de Recuperação
  - Completado a fase de análise, é preciso documentar os requisitos técnicos e de negócios para iniciar a fase de implementação.

Plano de recuperação de desastre

- A informação de ativos que você provavelmente precisará para desenvolver um DRP inclui:
  - O número, tipos e locais de mesas e outros móveis de escritório que podem ser usados para mobiliar um local secundário.
  - Pessoal necessário para o esforço de recuperação, junto com os dados para contato e as respectivas funções no processo de recuperação.
  - Software aplicativo e dados exigidos para funções críticas de negócios.
  - Recursos necessários para soluções manuais para contornar o problema.
  - Tempo máximo de interrupção e perda máxima de dados permitidos para cada aplicativo de software.
  - Periféricos exigidos, como impressoras, copiadoras, máquinas de faz e outros equipamentos de escritório.

Plano de recuperação de desastre

- Recuperação de desastre
  - É importante treinar todo o pessoal em relação à resposta apropriada a qualquer desastre.
  - As etapas críticas em responder a um desastre incluem:
    - Garantir a segurança de todos primeiro
    - Responder ao desastre antes de perseguir a recuperação
    - Seguir o DRP, incluindo comunicação com todas as partes afetadas.

Plano de recuperação de desastre

- Recuperação de desastre é uma extensão do DRP e trata de recuperação de defeitos ou de interrupções comuns de sistemas.
- Um desastre geralmente é maior que um defeito comum, e os recursos podem não estar disponíveis para cumprir soluções simples de recuperação.
- Um desastre pode inutilizar seu centro de dados, forçando-o a realocar suas operações. Um planejamento cuidadoso para tal mudança a tornará viável.

Plano de recuperação de desastre

- Muitas organizações permanecem despreparadas ou pouco preparada para um desastre, muitas sem possuir um DRP. Das que possuem, quase metade nunca testou seu plano - o que, basicamente, é o mesmo que não ter um.
- Os testes mais efetivos simulam desastres reais, incluindo transferir software entre sistemas computacionais e garantir que você possa estabelecer comunicações em um local alternativo.

Plano de recuperação de desastre

- Tipos de testes de DRP:
  - Teste de lista de verificação - Tipo mais simples, cada participante segue etapas na lista de verificação do DRP e fornece realimentação.
  - Revisão estruturada - Semelhante a um teste de lista de verificação, mas a equipe de DRP usa atuação em papéis para simular um desastre e avaliar a efetividade de um DRP.
  - Teste de simulação - Mais realista, a equipe de DRP usa atuações em papéis e segue com o máximo possível de efeitos de um desastre simulado sem afetar operações em andamento.
  - Teste paralelo - Avalia a efetividade do DRP, habilitando plena capacidade de processamento em um centro de dados alternativo, sem interromper o centro de dados principal.
  - Teste de interrupção completa - Interrompem o centro de dados principal e transferem a capacidade de processamento para um local alternativo.

Plano de recuperação de desastre

- Nem todo aspecto de um DRP é reativo. Algumas partes são preventivas e planejadas, acima de tudo, para evitar os efeitos negativos de um desastre.
- Componentes preventivos de um DRP podem incluir:
  - Espelhamento local de sistemas de disco e uso de tecnologia de proteção de dados, como RAID.
  - Protetores de surto para minimizar o efeito de surtos de alimentação em equipamentos eletrônicos delicados.
  - Fonte de alimentação ininterrupta e/ou gerador de energia.
  - Sistemas de prevenção de incêndio.
  - Software antivírus e outros controles de segurança.

Plano de recuperação de desastre

- Existem muitas abordagens para avaliar riscos. Cada organização conduz o processo de sua própria maneira.
- A seguir, serão apresentadas algumas metodologias disponíveis para efetuar o processo de avaliação de riscos.

Plano de recuperação de desastre

- Nome: Guia de Gerenciamento de Riscos para Sistemas de Tecnologia (*Risk Management Guide for Information Technology Systems* - NIST SP 800-30 e SP 800-66)
- Descrição: Parte dos relatórios da série Publicações Especiais (*Special Publication*) 800, estes produtos fornecem orientação detalhada sobre o que deve ser considerado em gerenciamento de riscos e avaliação de riscos em segurança de computador. Os relatórios incluem listas de verificação, gráficos, fórmulas e referências a edições regulamentadoras dos Estados Unidos. NIST SP 800-66 focaliza especificamente questões da HIPAA.
- Informações: www.csrc.nist.gov

Plano de recuperação de desastre

- Nome: Método de Análise e Gerenciamento de Riscos da CCTA (CCTA *Risk Analysis and Management Method*) - CRAMM
- Descrição: CRAMM é um método de análise de riscos desenvolvido pelo governo britânico. Melhores práticas de organizações do governo britânico são a base das primeiras versões do método e ferramenta CRAMM. Pessoas no mundo inteiro utilizam CRAMM. CRAMM é mais adequado para grandes organizações.
- Informações: www.cramm.com

Plano de recuperação de desastre

- Nome: Avaliação de Ameaças, Ativos e Vulnerabilidades Operacionalmente Críticas (*Operationally Critical Threat, Asset and Vulnerability Evaluation* - OCTAVE)
- Descrição: A abordagem OCTAVE define uma técnica de avaliação e planejamento estratégicos para segurança, baseada em risco. OCTAVE é uma abordagem autodirecionada. Existem duas versões de OCTAVE: OCTAVE e OCTAVE-S. OCTAVE é mais adequada para grandes organizações, enquanto OCTAVE-S funciona bem para organizações com menos de 100 pessoas.
- Informações: www.cert.org/octave/osig.html

Plano de recuperação de desastre

- Nome: ISO/IECC 27005 "Gerenciamento de Riscos de Segurança de Informação" ("*Information Security Risk Management*")
- Descrição: Um padrão ISO que descreve gerenciamento de riscos em segurança de informação de uma maneira genérica. Os documentos incluem exemplos de abordagens de avaliação de riscos de segurança de informação e listas de possíveis ameaças, vulnerabilidades e controles de segurança.
- Informações: www.iso.org

Referências

- Fundamentos de Segurança de Sistemas de Informação - David Kim. Michael G. Solomon