Disciplina: Segurança e Auditoria
Aula 2: Análise de Riscos

Professor: Rodrigo Rocha

Análise de Riscos
Agenda

- **Análise de Riscos**

- • Conceitos
- • Origem e classificação dos riscos
- • Fatores das categorias de Riscos
- • Origem e classificação dos riscos
- • Técnica de Análise de Riscos
- • Exemplos de técnicas de análise de riscos
- • Política de segurança

Risco

- **O que é?**
  - O risco é a relação entre a probabilidade e o impacto.
  - É a base para a identificação dos pontos que demandam por investimentos em segurança da informação.

- Os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas.

Origem e classificação dos riscos

- **Naturais:** são aqueles oriundos de fenômenos da natureza

- **Involuntários:** resultam de ações não intencionais, relacionados com vulnerabilidades humanas, físicas, de *hardware*, de *software*, dos meios de armazenamento e das comunicações;

- **Intencionais:** são aqueles derivados de ações deliberadas para causarem danos, e têm sua origem no ser humano.

Fatores das categorias de Riscos

- **Riscos naturais:**

  - 1- A área em que a empresa está instalada é sujeita a eventos da natureza, constantes ou não, de proporções catastróficas ou não;
  - 2- Falta de acompanhamento de boletins meteorológicos;
  - 3- Material empregado na construção de baixa resistência e/ou qualidade.
  - 4- Equipamentos de prevenção a sinistros (de origem na natureza) sem inspeção periódica e de má qualidade;
  - 5- Ausência de plano de recuperação de desastres e de continuidade dos negócios;
  - 6- Falta de treinamento em ações contingenciais.

Fatores das categorias de Riscos

- **Riscos involuntários**

  - 1- Falha nos equipamentos de prevenção e detecção;
  - 2- Descuido no cumprimento de normas para guarda, transporte e manuseio de material inflamável;
  - 3- Material de fácil combustão empregado na construção;
  - 4- Equipamentos ligados 24 horas;
  - 5- Ausência de treinamento em medidas contingenciais;
  - 6- Inexistência de processos de qualidade;
  - 7- Inexistência de controles internos;
  - 8- Inexistência de programa de capacitação continuada;
  - 9- Cultura organizacional.

Fatores das categorias de Riscos

- **Riscos intencionais**

  - 1- Situação do sistema de controle interno;
  - 2- Atratividade do produto e sua fácil receptação no mercado paralelo;
  - 3- Área em que a empresa está instalada sujeita a eventos da natureza de proporções catastróficas;
  - 4- Situação da criminalidade na região em que a empresa está instalada;
  - 5- Sensação de impunidade;
  - 6- Pagamento efetuado, em espécie, aos funcionários da empresa;
  - 7- Funcionários insatisfeitos com salários em atraso e sem perspectiva de continuidade no emprego;
  - 8- Mercado altamente competitivo;
  - 9- Informações de alto poder estratégico.

GERENCIAMENTO DE RISCOS

Conceitos

- É um processo voltado para o controle dos riscos e envolve um conjunto de atividades específicas que objetivam garantir a boa governança, sem que os riscos e surpresas indesejáveis atrapalhem o alcance dos seus objetivos e metas.

- Conjunto de métodos que permite identificar e analisar os riscos a que está submetida uma empresa, a quantificar as perdas derivadas de sua ocorrência, determinar as medidas ou meios precisos para eliminação e / ou redução dos mesmos , otimizando-as em termos econômicos.

- Compreende as atividades coordenadas para dirigir e controlar a organização em relação aos riscos.

Técnica de Análise de Riscos

- São métodos sistemáticos que auxiliam na identificação e análise dos riscos de uma atividade e estimam a probabilidade da ocorrência de evento indesejável.

- São técnicas reconhecidas mundialmente as elencadas a seguir:
  - Análise preliminar de risco – APR
  - Estudos de Identificação de Perigos **e Operabilidade - Hazop**
  - Análise dos Modos de Falhas e Efeitos - Amfe

Análise Preliminar de Riscos - APR

- Técnica de identificação de perigos e análise de riscos que consiste em identificar eventos perigosos, causas e consequências e estabelecer medidas de controle. Preliminarmente, porque é utilizada como primeira abordagem do objeto de estudo.

- Técnica que permite uma **Revisão Geral** dos riscos que estarão presentes nas fases operacionais, **categorizando-os para a priorização de ações preventivas e/ou corretivas.**

- **Aplicação :** Sistemas em início de desenvolvimento ou na fase inicial do projeto, quando apenas os elementos básicos do sistema e os materiais estão definidos.

Análise Preliminar de Riscos - APR

- Métodos

  - Definição dos objetivos e do escopo da análise.
  - Definição das fronteiras do processo/ instalação analisada.
  - Coleta de informações sobre a região, a instalação e os riscos envolvidos.
  - Subdivisão do processo/instalação em módulos de análise.
  - Realização da APR propriamente dita (preenchimento da planilha).
  - Elaboração das estatísticas dos cenários identificados por Categorias de Risco (frequência e severidade).
  - Análise dos resultados e preparação do relatório.

Estudos de Identificação de Perigos e Operabilidade - Hazop

- técnica de identificação de perigos e operabilidade que consiste em detectar desvios de variáveis de processo em relação a valores estabelecidos como normais. O objetivo do

- Tem por objetivo analisar os **Riscos Específicos** de uma planta de processo, bem como problemas operacionais que possam comprometer a **produtividade projetada.**

- Gera um elenco de medidas que permite a redução / eliminação dos riscos identificados e a diminuição de erros operacionais.

- É imprescindível em novos projetos, ampliações e novos estudos de unidades já existentes.

Estudos de Identificação de Perigos e Operabilidade - Hazop

- Métodos: O Hazop utiliza palavras-guia que estimulam a criatividade para detectar desvios.

Palavras-Guia	Desvios Considerados
Não, Nenhum	Negação do propósito do projeto. (ex.: nenhum fluxo)
Menos	Decréscimo quantitativo. (ex.: menos temperatura)
Mais, Maior	Acréscimo quantitativo. (ex.: mais pressão)
Também, Bem como	Acréscimo qualitativo. (ex.: também)
Parte de	Decréscimo qualitativo. (ex.: parte de concentração)
Reverso	Oposição lógica do propósito do projeto. (ex.: fluxo)
Outro que, Senão	Substituição completa. (ex.: outro que)

Análise dos Modos de Falhas e Efeitos - AMFE

- Visa detectar e controlar os **riscos oriundos de equipamentos**, identifica componentes críticos e gera uma relação de contra-medidas e formas de detecção precoce de falhas – especialmente útil em emergências de processos e utilidades.

- Promove aumento da confiabilidade do sistema pelo tratamento de componentes causadores de falhas de efeito crítico

- A AMFE é uma técnica de análise de riscos que consiste em **identificar os modos de falha dos componentes** de um sistema, os **efeitos dessas falhas** para o sistema, para o meio ambiente e para o próprio componente. O objeto da AMFE são os sistemas. O foco são os **componentes** e suas **falhas**.

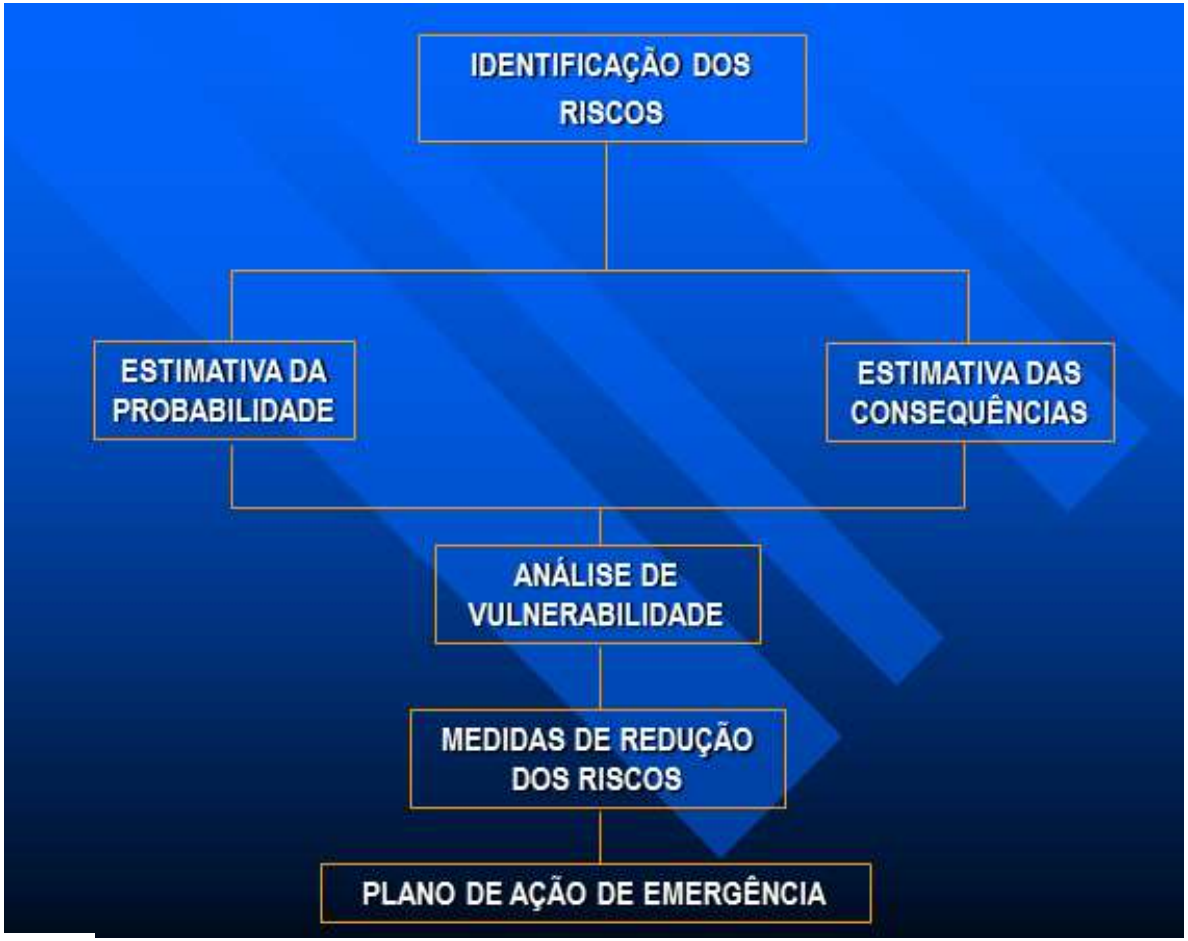
Análise dos Modos de Falhas e Efeitos - AMFE

- Métodos

  - Dividir o sistema em componentes;
  - Descrever as funções dos componentes;
  - Aplicar a lista de modos de falha aos componentes, verificando as falhas possíveis;
  - Verificar os efeitos das falhas para o sistema, o ambiente e o próprio componente;
  - Verificar se há meios de tomar conhecimento de que a falha está ocorrendo ou tenha ocorrido;
  - Estabelecer medidas de controle de risco e de controle de emergências.

Gerenciamento de Riscos

- Processo Básico



Gerenciamento de Riscos

- Avaliação do Sistema

Diretrizes de Gerência de Riscos

1. **Todo colaborador** deve levar em consideração todos os riscos dos quais possam resultar perdas humanas, materiais, financeiras e ambientais.

2. Compete a cada **gerente planejar, organizar, dirigir e controlar as atividades e recursos de sua responsabilidade**, de modo que consiga eliminar ou minimizar os riscos para a empresa.

3. Os resultados dos estudos elaborados de acordo com métodos pré-estabelecidos e as **decisões referentes à Gerência de Riscos deverão ser registradas por escrito.**

4. **Compete a cada gerente apontar todas as dificuldades e obstáculos técnicos, financeiros e administrativos que impeçam a implantação da Gerência de Riscos.**

Severidade da Frequência do Evento

Categoria	Denominação	Descrição/características
I	Desprezível	- Sem danos ou danos insignificantes aos equipamentos, à propriedade e/ou ao meio ambiente; - Não ocorrem lesões/mortes de funcionários, de terceiros (não funcionários) e/ou pessoas (indústrias e comunidade); o máximo que pode ocorrer são casos de primeiros socorros ou tratamento médico menor.
II	Marginal	- Danos leves aos equipamentos, à propriedade e/ou ao meio ambiente (os danos materiais são controláveis e/ou de baixo custo de reparo); - Lesões leves em empregados, prestadores de serviço ou em membros da comunidade.
III	Crítica	- Danos severos aos equipamentos, à propriedade e/ou ao meio ambiente; - Lesões de gravidade moderada em empregados, prestadores de serviço ou em membros da comunidade (probabilidade remota de morte); - Exige ações corretivas imediatas para evitar seu desdobramento em catástrofe.
IV	Catastrófica	- Danos irreparáveis aos equipamentos, à propriedade e/ou ao meio ambiente (reparação lenta ou impossível); - Provoca mortes ou lesões graves em várias pessoas (empregados, prestadores de serviços ou em membros da comunidade).

Classificação dos Riscos

Severidade		Frequência		Risco	
I	Desprezível	A	Extr. Remota	1	Desprezível
II	Marginal	B	Remota	2	Menor
III	Crítica	C	Improvável	3	Moderado
IV	Catastrófica	D	Provável	4	Sério
		E	Frequente	5	Crítico

Matriz de Riscos

Probabilidade / Impacto	Sem Impacto	Leve	Médio	Grave	Gravíssimo
Quase certo	Risco Elevado	Risco Elevado	Risco Extremo	Risco Extremo	Risco Extremo
Alta	Risco Moderado	Risco Elevado	Risco Elevado	Risco Extremo	Risco Extremo
Média	Risco Baixo	Risco Moderado	Risco Elevado	Risco Extremo	Risco Extremo
Baixa	Risco Baixo	Risco Baixo	Risco Moderado	Risco Elevado	Risco Extremo
Raro	Risco Baixo	Risco Baixo	Risco Moderado	Risco Elevado	Risco Elevado

Exemplo da Matriz de Riscos

Item	R / O	Fase	Risco Descrito	Consequências	Probabilidade (Alta, Média ou Baixa)	Impacto (Alto, Médio ou Baixo)	Severidade (Ver matriz de severidade)	Categoria de Resposta (Acceptance, Mitigation, Transference e Avoidance)	Procedimento para Resposta
10	R	Planejamento	Dificuldade na identificação da maior necessidade da instituição	Atraso no cronograma, possível perda de qualidade no projeto	Médio	Médio	Médio	Mitigar	Procurar fornecedores para mais de um dos bens possíveis e alinhar com a instituição sobre a necessidade de cada um
20	R	Planejamento	Dificuldade de comunicação com a instituição	Atraso no cronograma, possível perda de qualidade no projeto	Médio	Médio	Médio	Mitigar	Divulgação das atividades realizadas ao responsável, alinhamentos periódicos
30	R	Planejamento	Dificuldade no levantamento de fornecedores do bem a ser adquirido	Atraso no cronograma	Baixo	Alto	Médio	Mitigar	Iniciar etapa antes mesmo da definição do bem a ser adquirido, abrindo possibilidades de mudanças; pesquisa e avaliação de fornecedores.
40	R	Planejamento	Falha no orçamento do projeto	Aumento de custos, atrasos no cronograma, não atingimento de metas, possível prejuízo	Baixo	Alto	Médio	Mitigar	Avaliação de fornecedores, orçamentos detalhados, antecipação das compras
50	R	Execução	Arrecadação inferior ao orçamento do projeto	Aumento de custos, atrasos no cronograma, não atingimento de metas, possível prejuízo	Médio	Alto	Alto	Mitigar/Transferir	Divulgação entre pares e em redes sociais. Além disso, os membros do grupo realizariam os pagamentos das cotas integrais em caso de não conseguirem vender as rifas
60	R	Planejamento	Falta de estoque para os prêmios da rifa	Atraso no cronograma, Aumento de custos	Baixo	Médio	Baixo	Mitigar	Compra antecipada dos itens de rifa
70	R	Planejamento	Variação de preço dos prêmios da rifa	Atraso no cronograma, Aumento de custos	Médio	Médio	Médio	Mitigar	Compra antecipada dos itens de rifa
80	R	Planejamento	Falta de atratividade dos prêmios da rifa	Aumento de custos, atrasos no cronograma, não atingimento de metas, possível prejuízo	Médio	Médio	Médio	Mitigar	Estudo de atratividade de produtos entre possíveis compradores (amigos, familiares, colegas de trabalho)

Planilha de APR

Empresa:
Processo:
Intenção Projetada:

Risco	Possíveis Causas	Consequências	Categoria			Ações Requeridas
			Freq.	Sever.	Risco	

Exemplo de APR

- Conta a mitologia grega que o Rei Minos, de Creta, mandou aprisionar Dédalo e seu filho Ícaro, na parte montanhosa da ilha.
- Com objetivo de escapar da Grécia Dédalo idealizou fabricar asas; o que fez habilidosamente com penas, linho e cera de abelhas.
- Antes da partida, Dédalo advertiu a Ícaro que tomasse cuidado quanto a seu curso:
  - • Se voasse muito baixo, as ondas molhariam as penas;
  - • Se voasse muito alto, o sol derreteria a cera e ele cairia no mar;
  - E ele cairia no mar!
- Essa advertência, uma das primeiras análises de riscos que se pode citar, define o que hoje chama-se Análise Preliminar de Riscos - APR.

Exemplo da Planilha de APR

Empresa: DÉDALO E ÍCARO ME
Processo: FUGA DE CRETA
Intenção Projetada: VOAR UTILIZANDO ASAS.

Risco	Possíveis Causas	Consequências	Categoria			Ações Requeridas
			Freq.	Sever.	Risco	
1- Radiação térmica do sol	-Voar muito alto em presença de forte radiação.	1.1- O calor derrete a cera que une as penas: Não sustentação aerodinâmica, aeronauta pode morrer no mar.	D	IV	5	1.1.1- Prover orientação quanto a vôo muito alto. 1.1.2- Restringir área da superfície aerodinâmica com linho, entre aeronautas.
2- Umidade elevada	- Voar muito perto da lamina d'água	2.1- Asas absorvem água aumentando peso do conjunto – aeraonauta pode morrer no mar	D	IV	5	2.1.1- Advertir aeronauta para voar a meia altura – o sol mantêm as asas secas.

EXEMPLO DE HAZOP

Quadro 11 - Planilha de HAZOP

Sistema: Transferência de Produto Corrosivo do Caminhão para o Tanque			**Equipe:**		**Data:**
Parâmetro: vazão		**Nó:** 01			**Página:** 1/4
Palavra Guia	**Desvio**	**Causas**	**Detecção**	**Conseqüências**	**Providências**
Mais	Mais Vazão	• Falha no arqueamento do tanque; • Caminhão com quantidade de produto maior do que o tanque comporta; • O tubo de inspeção não é vedado; • O dreno do tanque está entupido; • O dreno do tanque está mais alto do que o topo do tubo de inspeção.	Visual	• Transbordamento do tanque de ácido com perda de produto; • Danos a estrutura do tanque; • Danos aos equipamentos atingidos; • Geração de resíduos químicos; • Gastos na manutenção do tanque e equipamentos; • Gastos na descontaminação do local; • Projeção de ácido sobre o comando das bombas.	• Instalação de um medidor de nível para o tanque; • Instalação de chaves LSH e LSHH; • Envio da nota fiscal do Almoxarifado para o operador da ETA, para checar se a quantidade de ácido do caminhão é a quantidade requisitada; • Elevar o tubo de inspeção; • Vedar o tubo de inspeção com tampa rosqueada e juntas "o-ring"; • Relocar botoeiras de comando.

FATORES CRÍTICOS DE SUCESSO

- Importantes para o sucesso do gerenciamento de riscos

  - O patrocínio da diretoria da organização;
  - A definição dos requisitos do gerenciamento alinhado com a missão e os objetivos da empresa;
  - O estabelecimento do escopo de todo o processo;
  - O ambiente das atividades de negócios e a criticidade do produto;
  - A definição de uma equipe multidisciplinar para o macroprocesso e suas responsabilidades definidas;
  - A definição dos colaboradores de diversas áreas da organização e as suas atribuições no processo;

FATORES CRÍTICOS DE SUCESSO

- Importantes para o sucesso do gerenciamento de riscos

  - A forma da comunicação interna;
  - A cultura da segurança da informação;
  - A identificação dos principais ativos e processos de negócios;
  - A confiabilidade da lista das principais ameaças à segurança da informação;
  - A escolha e a utilização do método de análise dos riscos;
  - Os critérios de parametrização para a classificação dos riscos e as medidas de tratamento;
  - A implementação das medidas para o tratamento dos riscos;
  - O controle e o monitoramento constante do processo.

Benefícios

- Poucas surpresas;
- Exploraç… …to
  des…
- P…
- T…
  exat…
- Manutenç…
- Proteção dos diretores;
- Responsabilidade, garantia e governança; e
- Bem-estar pessoal.

Garantir o desenvolvimento das atividades de negócios dentro de um ambiente de controle permanente sobre os riscos

Políticas de Segurança da Informação

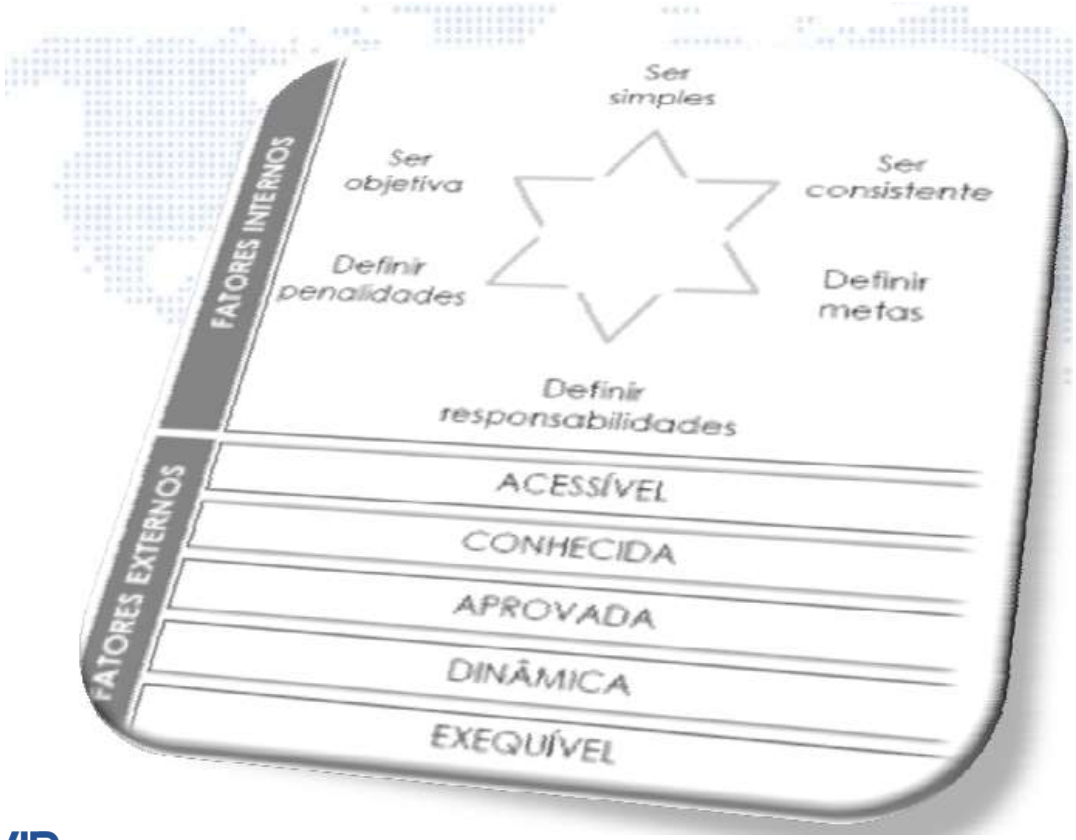
- **Política de segurança?**

  - A política de segurança da informação (PSI) deve estar alinhada com os objetivos de negocio da organização

  - Ela é estruturada em:
  - • Diretrizes
  - • Normas
  - • Procedimentos

Política de Segurança

- A política possui características, ou fatores, internos e externos, que precisam ser respeitados por ocasião de sua elaboração e implementação.



Classificação da Informação

As informações possuem valor e usos diferenciados, e portanto, precisam de graus diferenciados de proteção.

Cada tipo de proteção possui seu próprio custo, e classificar a informação é um esforço para evitar o desperdício de investimento ao se tentar proteger todas a informação.

Classificação da Informação

- A informação deve ser classificada em nível corporativo, e não por aplicação ou departamento. Os principais ganhos são:

  - A CID é fortalecido pelos controles implementados em toda a organização;
  - O investimento em proteção é otimizado;
  - A qualidade das decisões é aumentada, já que as informações são mais confiáveis;
  - A organização controla melhor suas informações e pode fazer uma re-analise periódica de seus processos e informações.

Dúvidas... Sugestões...

Dúvidas?

Sugestões?