Capítulo 3

3 Modelo Reason de acidente organizacional

Em 1997, o professor James Reason contribuiu com estudos e pesquisas relacionados ao gerenciamento de risco nas empresas, ao lançar a proposição de que fatores associados à organização e à gestão contribuem maciçamente para a ocorrência dos acidentes nas organizações, constituindo falhas latentes dos sistemas de trabalho, tal qual aos agentes patogênicos residentes nos sistemas biológicos.

Esses acidentes organizacionais, segundo Reason (2006), são produtos dos tempos recentes e frutos das inovações tecnológicas que vieram alterar radicalmente a relação sistemas x ser humano. Ao observá-los, Reason (2006) notou que os acidentes organizacionais têm freqüência rara, causas diversas, envolvem todos os níveis hierárquicos da organização, conseqüências que podem atingir toda a população (relacionada à empresa) e o meio ambiente, e são resultados de eventos difíceis de compreender, controlar e prever.

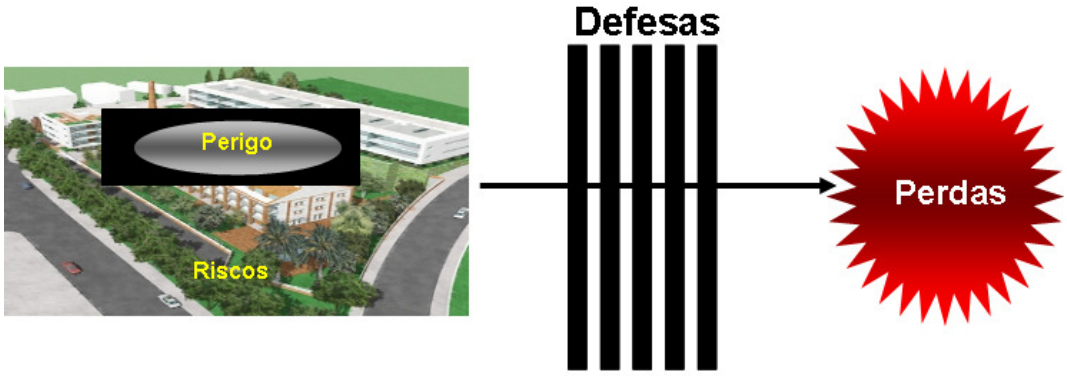
Ao acreditar que existe uma explicação lógica para a ocorrência dos acidentes organizacionais, sendo somente acidentais no modo que vários fatores combinam para gerar o mesmo, e que não existe nada acidental na existência desses precursores, Reason (2006) buscou encontrar um modelo que pudesse ser aplicado igualmente bem para um amplo leque de opções, desde baixos riscos até domínios altamente perigosos.

Partindo dessa premissa, Reason (2006) mostrou que todo acidente organizacional é fruto do rompimento de barreiras e proteções que separam os perigos e avarias das pessoas ou ativos – chamados por ele de perdas, conforme a Figura .

O porquê das falhas das defesas é, segundo o autor, a participação de três conjuntos de fatores – humano, técnico e organizacional – administrados por dois processos comuns a todas as organizações: produção e proteção.

Como toda organização requer várias formas de proteção para mediar entre os perigos locais e suas possíveis perdas, e como os recursos que fazem a proteção possível são oriundos da produção, esta tem prioridade em relação à proteção na

maior parte do ciclo de vida da organização. Por isso, a parceria entre produção e proteção é raramente igual, e um dos processos predominará, dependendo das circunstâncias, conforme o referenciado autor.



Fonte: Reason, 2006
Figura 6 - O relacionamento entre perigo, defesas e perdas

Além do mais, uma proteção de sucesso é indicada pela ausência de resultados negativos. Somente após um acidente ou um incidente grave é que a proteção aparece – por um breve período – na memória daqueles que administram as organizações, quando então, freqüentemente durante o período imediatamente após um mau evento, melhorias na proteção são colocadas em prática. Embora o objetivo seja evitar a repetição de um acidente, essas melhorias nas defesas acabam conferindo vantagens produtivas, e o aumento de produção adicional eleva a organização ao mesmo nível de proteção inadequada que existia antes do evento. Este processo é chamado de "compensação do risco" (REASON, 2006).

O retorno a um nível de proteção inadequado acontece porque tanto a preocupação em garantir determinados níveis de segurança existe por um curto espaço de tempo, quanto um longo período sem ocorrência de um acidente leva as organizações a correrem o risco de atravessar um estado de "erosão da proteção" em favor dos ganhos produtivos.

Essa situação típica ocorre, segundo Reason (2006), pela falibilidade humana de esquecer o medo das coisas que raramente acontecem, particularmente quando as organizações têm de enfrentar imperativos produtivos, tais como o crescimento, lucros e competitividade.

O aumento da produção sem o correspondente aumento dessas medidas vai reduzir as margens de segurança existentes e, se em curto prazo não traz conseqüências negativas, fazendo parte da rotina de trabalho, gradualmente leva a um estado de redução/erosão das margens de segurança, em favor dos ganhos

produtivos, tornando o contexto organizacional vulnerável a combinações particulares de fatores causadores de acidentes, comparados por Reason (2006) a um "*unrocked boat*". É importante lembrar que esses fatores causadores de acidentes ocorrem quase que diariamente, quando administradores e supervisores de linha têm que escolher se devem ou não romper barreiras de segurança para alcançar os objetivos ou outras demandas operacionais.

Como resultado destas imposições, o investimento em efetivas medidas de proteção e a tendência para preservar as medidas já existentes decrescem, desencadeando uma redução das margens de segurança do sistema, com um conseqüente aumento do risco.

As **medidas de proteção (defesas do sistema)** estão relacionadas com o(s) mecanismo(s) de proteção das pessoas e máquinas de modo a evitarem lesões ou danos inerentes às atividades produtivas. As medidas de proteção são classificadas, segundo Reason (2006), de acordo com:

I. O seu modo de aplicação:
   a. As *hard* - garantem as funções de alerta (os alarmes e dispositivos de alerta e de informação de perigos associados a determinados locais ou situações) e incluem: as barreiras de segurança (permitem afastar o homem do perigo), os equipamentos de proteção individual e as formas de contenção de perigos que não possam ser eliminados pelas barreiras;
   b. As *soft* - relacionadas com a "combinação de papel e pessoas", onde estão incluídos: a legislação que regulamenta os aspectos da segurança; os procedimentos de segurança com orientações claras; as formas de restabelecimento do estado de segurança ou normalidade do sistema, após situação anormal; os meios ou planos de evacuação previamente definidos face à falha de mecanismos de retenção de perigos; a supervisão e os operadores propriamente ditos.

II. Funções que exercem:
   a. Tomar ciência e advertir da proximidade do perigo eminente;
   b. Orientar como operar seguramente;
   c. Alarmar e avisar quando o perigo for eminente;
   d. Restaurar o ambiente para um estado seguro;
   e. Interferir com barreiras de segurança entre o perigo e as perdas potenciais;

f. Conter e eliminar o perigo caso escape das barreiras;
g. Prover escape e resgate.

Nesta descrição da natureza das medidas de proteção está implícita a hierarquização da prevenção a qual Reason (2006) designa de "*defences-in-depth*" - sucessivas barreiras de proteção, uma após outra, cada uma salvaguardando contra a possível ruptura da barreira à frente. "*Defences-in-depth"* tem suas vantagens e suas desvantagens. Uma das conseqüências infelizes é que tornam o sistema mais complexo e cada vez mais opaco para as pessoas que gerenciam e operam o mesmo, o que permite a incidência do surgimento de condições latentes.

3.1 Modelo "queijo suíço" de defesa

Em um mundo ideal, as barreiras de proteção, criadas pelas medidas de proteção adotadas, deveriam estar intactas, não sendo permitida nenhuma penetração por possíveis acidentes, segundo Reason (2006). Porém, no mundo real cada barreira tem brechas e deficiências - os buracos, que são as falhas ativas e as condições latentes. Essas barreiras admitem o surgimento de buracos em cada uma delas, mesmo permitindo adaptações às condições locais e remoções quando necessárias, como resultado dos imperativos produtivos já descritos anteriormente.

Reason (2006) comparou esses buracos nas medidas de proteção a um "queijo suíço", conforme pode ser observado na Figura 7. Em uma organização todas as medidas de proteção são representadas por um conjunto de camadas ligadas entre si, por ordem de prioridade, impossibilitando a passagem da "trajetória" que "desenha" o acidente. Porém, numa situação real, estas camadas defensivas apresentam buracos que se encontram num fluxo contínuo.

As condições latentes existem a qualquer nível organizacional e ficam presentes durante muito tempo na organização, adormecidas, antes de se combinarem com as circunstâncias locais e falhas ativas e penetrarem nos "buracos" alinhados das camadas defensivas existentes no sistema.

A idéia base do modelo de queijo suíço desenvolvido por Reason (2006) é de que os erros, além de poderem ser desencadeados pelos operadores, também o vão sendo em diferentes níveis hierárquicos de uma organização, assumindo

diferentes formas e conseqüências. Identificar as falhas que ocorrem em vários níveis hierárquicos auxilia na identificação das medidas corretivas adequadas.

Fonte: Reason, 2006
Figura 7 - Modelo queijo suíço

De um modo geral, uma premissa comum a diversos modelos de análise na causalidade de buracos é a distinção entre as falhas humanas, cujos efeitos se manifestam quase imediatamente – falhas humanas ou ativas - e aquelas cujos efeitos podem permanecer adormecidos no seio de uma organização, por períodos de tempo mais ou menos longos – condições latentes. A distinção entre falhas ativas e condições latentes está resumida no Quadro 1.

(1) **Condições latentes -** São aspectos diretos e observáveis no modo como os sistemas de trabalho funcionam e cujas conseqüências adversas não são imediatas, podendo permanecer ocultas durante um certo tempo tornando-se evidentes quando se combinam com circunstâncias locais e falhas ativas para penetrar nas muitas barreiras de defesa do sistema. Estão presentes em todos os sistemas, sendo uma inevitável parte da vida organizacional. São exemplos de condições latentes: *design* inadequado dos equipamentos face às exigências operacionais; falhas na supervisão e manutenção; procedimentos de trabalho deficientes; estratégias ou tomadas de decisões não adequadas ao nível dos fabricantes, projetistas e gestores das organizações, falta de treino (ou este ser não apto), de ferramentas e de equipamento; ou simplesmente, serem resultado de erros e violações.

(2) **Falhas ativas ou humanas –** São as falhas que têm efeitos imediatos e as suas conseqüências são imediatamente posteriores ao desenrolar do acidente. Manifestam-se através de erros e violações cometidos por

> uma parte da organização que é constituída, geralmente, pelos elementos expostos aos mais severos perigos - os operadores. Estão, portanto, associadas aos operadores ou em comando ou em contato direto com o sistema produtivo.

Deste modo, para um acidente organizacional acontecer é necessária uma conjunção rara de um conjunto de buracos nas camadas defensivas sucessivas, permitindo a aproximação do risco em um contato perigoso com as pessoas e os ativos – as "janelas de oportunidade", isto é, o alinhamento das "aberturas" ou fraquezas nas camadas defensivas, sugerindo que sobre os elementos básicos de todo e qualquer sistema produtivo ou organização ocorrem falhas ou erros que podem constituir condições latentes que, por sua vez, aliadas aos erros de *performance* contribuem para o desencadear do acidente.

Para Reason (2006), as más decisões e os procedimentos de trabalho deficientes, que são um reflexo dos erros de juízo por parte dos elementos "decisores", acabam por se converter em formas de trabalho normalizadas, e apesar de não terem conseqüências imediatas nem se manifestarem de modo imediato, apresentam vulnerabilidades fundamentais que constituem as circunstâncias (condições latentes), que a dado momento e de forma involuntária se combinam com a ação humana (falhas ativas) e provocam diretamente o acidente.

Deste modo, o modelo do "queijo suíço" proposto por Reason (2006) auxilia numa melhor compreensão da gênese do acidente, salientando e descrevendo a importância e a forma de envolvimento dos fatores humanos nas circunstâncias imediatamente anteriores ao acidente, na medida em que as condições latentes surgem a partir de falhas ao nível de tomada de decisões; das deficiências ao nível das linhas de gestão; das condições preexistentes ou precursores psicológicos.

Já em face de um acidente, toda a organização deve se questionar sobre a relação dos seus pressupostos de segurança e as práticas organizacionais, e assim introduzir mudanças futuras. Estudar um acidente, assim como estudar os fatos históricos, mesmo tendo seus recursos e disponibilidade de evidências confiáveis limitados é importante por duas razões: para estabelecer o que ocorreu e para evitar que se repita no futuro.

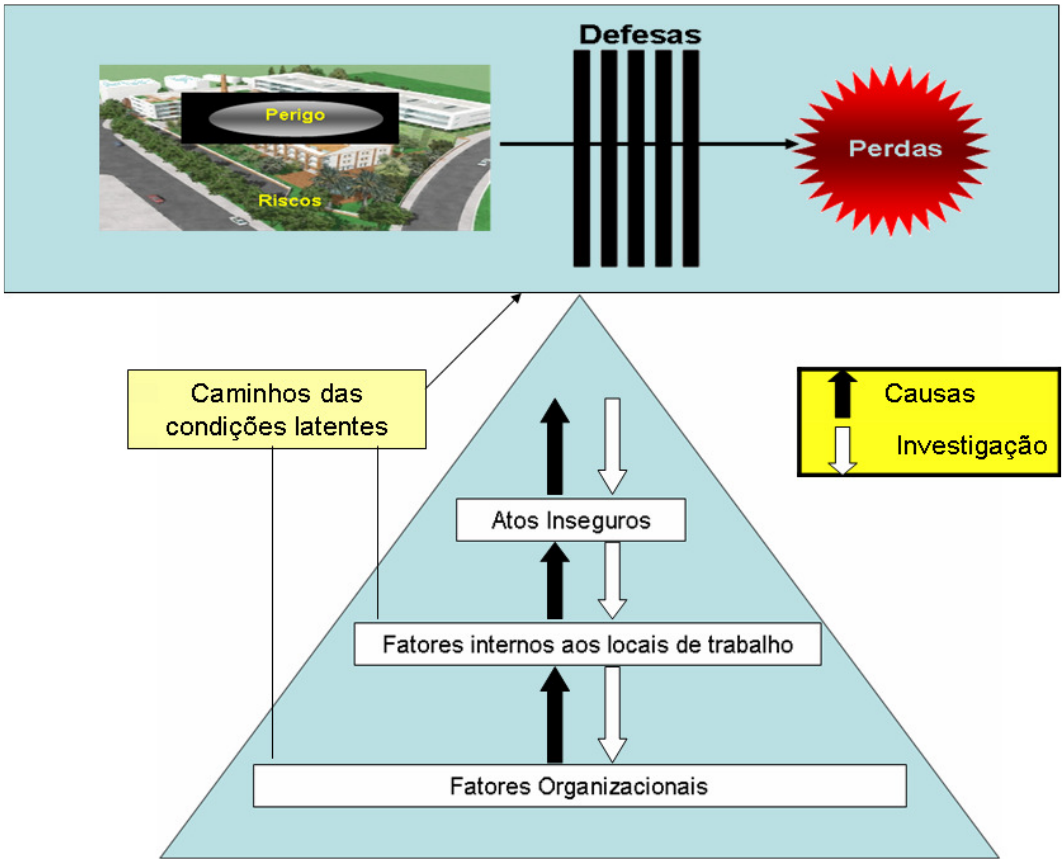
Falhas ativas/humanas	Condições latentes
O impacto adverso é de efeito imediato.	Pode manter-se latente durante algum tempo sem que haja efeito lesivo.
Cometidas por aqueles que se encontram na linha da frente.	Localizadas nos altos cargos de uma organização e relacionadas com a produção, regulamentação e agências governamentais.
Tende a ser única para um efeito específico.	Podem contribuir para um diferente número de acidentes.
---	Podem favorecer: a criação de fatores locais promotores de erros e violações e agravar as conseqüências dos atos inseguros, pelos efeitos sobre as medidas de proteção do sistema (barreiras, proteções,...).

Fonte: Reason, 2006
Quadro 1 - Falhas ativas x condições latentes

Por isso, e porque a quantidade e confiabilidade das informações relevantes se deterioram rapidamente com o passar do tempo da ocorrência do evento, uma ferramenta para se entender as causas de um acidente é proposta pelo referido autor (ver Figura 8), para ser utilizada restritamente às fronteiras organizacionais da organização questionada.

A ferramenta apresentada busca associar os vários elementos contribuintes de um acidente em uma seqüência coerente que funciona de baixo para cima em termos de causalidade, e de cima para baixo em termos investigativos.

Portanto, a história da causa começa com os fatores organizacionais: decisões estratégicas, processos organizacionais genéricos – demanda, recursos alocados, planejamento, comunicação, gerenciamento, auditoria, e outros. São esses processos que mapeiam e colaboram a cultura organizacional, incluindo as atitudes não faladas e as regras não escritas. Embora os atos inseguros estejam comprometidos com os acidentes organizacionais, eles não são condições necessárias para a causa do acidente. Em algumas ocasiões, as defesas falham simplesmente como resultado de condições latentes.



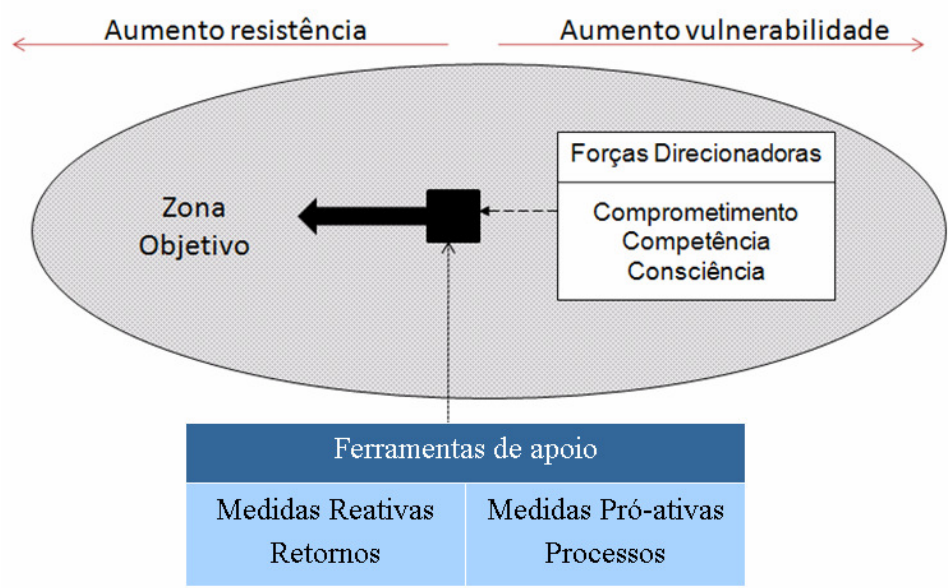
Fonte: Reason, 2006
Figura 8 - Modelo das causalidades

Já para analisar ou investigar um acidente, a direção é a oposta à das causas. A investigação deve começar com o evento ruim e em seguida considerar como e quando as defesas falharam:

- Para cada defesa furada ou passada, é necessário estabelecer quais falhas ativas e condições latentes estavam envolvidas;
- Para cada ato inseguro identificado, deve-se considerar quais condições locais moldaram ou propiciaram o mesmo.
- Para cada uma dessas condições locais, deve-se perguntar qual fator organizacional superior contribui para tal, sendo que uma única condição local pode ter sido provocada por mais de um fator organizacional, por causa da rede de processos existente entre o local de trabalho e o topo da organização.

3.2 O espaço de segurança

O espaço de segurança é um espaço imaginário usado para representar a atual resiliência ou vulnerabilidade de uma organização. Sua representação gráfica pode ser observada na Figura 9.



Fonte: Reason, 2006
Figura 9 - Resumo dos principais fatores envolvidos na navegação do espaço de segurança

Reason (2006) afirma que muitos fatores diferentes agem para determinar a posição bidimensional de segurança/insegurança de uma organização, posição esta que deve ser fruto da qualidade do processo usado para combater os perigos operacionais, isto é, ser uma função da extensão e integridade de suas defesas em um dado momento.

Mesmo que a posição ocupada no espaço bidimensional por uma organização possa demonstrar segurança absoluta, isso pode não ser verdadeiro, pois com os perigos naturais, a falibilidade humana, as condições latentes e a possibilidade de mudanças nas conjunturas dos fatores que provocam acidentes continuarão a existir, mesmo as organizações mais resilientes podem ainda ter acidentes. Da mesma forma, organizações sortudas, mas inseguras, podem ainda escapar de acidentes por um longo período de tempo.

Ainda segundo o citado autor, muito poucas organizações ocupam espaços fixos dentro do espaço de segurança, a maioria se encontra em movimento contínuo. Quanto mais a organização se aproxima de uma ou de outra

extremidade do espaço de segurança, mais intensas são as forças que fluirão naturalmente em direções opostas no espaço. Por isso, os acidentes são importantes para, mesmo temporariamente, se lembrar das questões de proteção mais do que as de produção. Quando uma organização se torna insegura e, desse modo mais vulnerável a acidentes, as pressões reguladoras e públicas se tornam mais intensas e juntamente com a memória recente de um acidente, pressionam para um aumento das medidas de segurança necessárias.

Do mesmo modo, à medida que uma organização se torna mais segura, as medidas de segurança perdem a sua força, perde-se o medo e passa-se a dar mais atenção e recursos aos objetivos de produção, retornando ao ciclo vicioso proteção/produção.

Portanto, para Reason (2006), um gerenciamento de segurança efetivo significa navegar ativamente no espaço de segurança para alcançar e tentar continuar dentro da zona de resiliência máxima, compreendendo tanto a natureza das forças que agem sobre a organização quanto o tipo de informação necessária para fixar a posição atual. Para esse gerenciamento efetivo aconselha-se a utilização de um "instrumento" interno de segurança que conduza a organização na direção certa, e ferramentas auxiliares para assinalar seu progresso.

Reason (2006) também identifica três forças direcionadoras do instrumento de segurança, que ele chamou de "três Cs":

(a) **Comprometimento** – seja por motivação, relacionado às questões de domínio do modelo de boas práticas de segurança ou de se manter um passo a frente dos agentes reguladores, e/ou pelos recursos, alocados para atingir os objetivos de segurança, de qualidade, com quantidade, valorizados;

(b) **Competência** - relacionada com a qualidade dos sistemas de informações de segurança da organização, coletando, disseminando e influenciando as decisões;

(c) **Consciência** - dos riscos que rondam suas operações. Uma organização consciente vê a "guerra da segurança" como ela realmente é: uma longa batalha com nenhum final conclusivo de vitória. Um período longo sem acidentes não significa a paz, mas sim um período onde se devem reforçar os cuidados.

A essência para um bom gerenciamento de segurança, segundo Reason (2006), está em saber o que é gerenciável e o que não é; saber que só se pode defender e não remover ou evitar os riscos; lutar para minimizar os atos inseguros e não os eliminar todos de uma só vez. Ao invés de tentar exercer o controle direto sobre os incidentes e acidentes, deve-se regularmente medir e melhorar os processos que reconhecidamente se relacionam com a ocorrência dos acidentes organizacionais.

As **medidas reativas** só podem ser aplicadas depois de uma ocorrência de um evento. A coleta e análise dos relatórios de incidentes[1] são importantes nessa ferramenta, pois os incidentes ocorrem mais freqüentemente do que retornos ruins. Ambos provêem, também, visões qualitativas de como pequenas falhas na defesa podem criar grandes desastres, fornecendo números necessários para uma análise quantitativa mais profunda e uma lembrança poderosa dos perigos que rondam o sistema, reativando a sensação de medo.

Para tal, toda a informação obtida deve ser disseminada na organização, juntamente com uma estimativa realista do potencial custo financeiro de perda que a mesma traria. É a partir da visão exata da fragilidade e ausências existentes nas barreiras de defesa que as medidas reativas são utilizadas, então, como "vacinas" para mobilizar o sistema de defesa contra ocorrências mais sérias no futuro.

As **medidas proativas** são medidas preventivas, que devem ser adotadas antes que um evento ruim aconteça. Seu propósito é obter amostras de índices que reflitam o estado atual, em termos de vulnerabilidade, dos vários processos organizacionais, identificando os que necessitam mais urgentemente de reforço nas medidas de proteção. Provêem, ao mesmo tempo, checagem regular tanto nas defesas do sistema quanto nos "sinais vitais" em níveis organizacionais e locais.

A freqüência com que deve ser feito o monitoramento varia conforme a taxa de variação obtida dos mesmos, sendo que, normalmente, os fatores locais precisam ser monitorados em intervalos mais freqüentes, pois mudam mais rapidamente do que os organizacionais. Três áreas devem ser observadas e avaliadas para cada processo identificado:

(a) **Os atos inseguros** (fator humano) - buscando informações relacionadas com a natureza (erro ou violação) e variedade dos

[1] Ou *near-miss* é um evento que poderia ter tido uma conseqüência ruim, mas não teve.

mesmos, pois diferentes atos inseguros requerem diferentes tipos de gerenciamento;

(b) **Os fatores locacionais** de trabalho - precursores mentais e físicos dos atos inseguros, mais fáceis de serem gerenciados (por serem em menor número), são somente expressões locais de problemas organizacionais de um nível mais elevado;

(c) O**s fatores organizacionais** - representam a área prioritária para a medição dos processos, pois se as falhas nesse nível não forem corrigidas, não adianta as mudanças feitas em nível tanto locais como do trabalhador, porque as falhas voltarão e serão substituídas por outros problemas locais e humanos.

3.3 Modelo regulador de gerenciamento do erro

Reason (2006) identifica o gerenciamento do erro como tendo dois componentes: (a) redução do erro, compreendendo medidas para limitar a ocorrência de erros, e (b) retenção do erro, uma vez que a redução nunca terá êxito completo, são necessárias medidas desenvolvidas para limitar as conseqüências adversas dos erros que ainda ocorram. Observa, também, que a maior parte das tentativas de gerenciamento do erro é feita mais reativa do que pró-ativa, direcionada mais a um evento do que direcionada a um princípio.

Para o autor, uma ferramenta de gerenciamento do erro deve incluir medidas para:

(a) Minimizar a probabilidade de ocorrência de erros de um indivíduo ou de uma equipe;

(b) Reduzir a vulnerabilidade de uma dada tarefa ou elemento da tarefa;

(c) Descobrir, acessar e eliminar fatores de produção de erros (e os de violação) nos locais de trabalho;

(d) Diagnosticar fatores organizacionais que geram fatores produtores de erro nos indivíduos, equipes, tarefas ou locais de trabalho;

(e) Garantir a detecção de erro;

(f) Aumentar a tolerância a erros dos locais de trabalho ou do sistema;

(g) Tornar as condições latentes mais visíveis para aqueles que operam e gerenciam o sistema;

(h) Melhorar a resistência intrínseca à organização e às falibilidades humanas.

Para o autor, os erros são moldados e provocados pelos fatores organizacionais e locais de trabalho superiores e que sua identificação é meramente o início da busca das causas, não o fim. O erro, assim como o desastre que pode se seguir dele, é algo que requer uma explicação. Somente ao compreender o contexto que provoca o erro pode-se limitar sua recorrência.

Segundo o mesmo, existem várias ferramentas no mercado que tratam do gerenciamento do erro e que são muito utilizadas, tais como: Gestão da qualidade total (TQM - T*otal Quality Management*); Análise de tipo e efeito da falha (FMEA - *Failure Mode and Effect Analysis*); Árvore de falha (FTA - F*ailure Tree Analyis*); Análise da confiabilidade humana (HRA - H*uman Reliability Analysis*); Análise dos erros humanos (HEA - H*uman Error Analysis*); Diagrama de espinha de peixe (*Fishbone).*

Porém, para Reason (2006), a maioria dessas ferramentas enfoca seus recursos no acidente individual, e como tal faz parte de um *kit* de ferramentas essencial para o gerenciamento de risco com enfoque mais organizacional.

O enfoque, segundo o autor, deve ser em ferramentas pró-ativas e reativas de gerenciamento de erro que trabalhem o acidente organizacional, e permitam revelar e corrigir os fatores produtores de erro, tanto no local de trabalho como organizacional, compostas por três elementos:

I. Uma filosofia de segurança coerente que leve a um cenário de objetivos de segurança alcançáveis;

II. Uma maneira integrada de pensar sobre os processos que interrompem uma operação segura;

III. Um conjunto de instrumentos para medir esses processos de interrupção – chamado, pelo autor, de falhas nas situações de trabalho (GFT – *general failure types*) – que não dependam de estatísticas de acidentes ou incidentes, i.e., das medidas de retorno.

Para Reason (2006), a filosofia de gerenciamento de erro organizacional proposta deve:

(a) Focar o gerenciamento de risco como essencialmente um problema de controle organizacional;
(b) Ter a habilidade de saber o que é controlável e o que não é;
(c) Saber que os atos inseguros, quase-acidentes[2] e acidentes surgem da união das deficiências nas situações de trabalho e fatores desencadeadores locais;
(d) Saber que somente antecipando e corrigindo as GFT é a única maneira de se evitar quase-acidentes;
(e) Que um gerenciamento de risco efetivo depende de medidas regulares e reparação seletiva das GFTs.

Por isso a medição e o controle das GFTs são muito importantes no gerenciamento de erro. Para Reason (2006), a identificação das GFTs pode ser feita em parte pela recorrência das condições latentes associadas aos eventos passados, e pelas novas condições criadas pelas mesmas, que promovem ou agravam os atos inseguros. Os indicadores ou sintomas da presença e grau de cada GFT podem ser obtidos diretamente dos especialistas na tarefa a serem executadas.

O autor também incentiva a utilização de fiscais ou reguladores do risco para monitoramento e identificação das práticas insatisfatórias e equipamentos pobres que as empresas cresceram acostumadas a trabalhar.

Normalmente são especialistas, treinados periodicamente e com vasta experiência na identificação de insuficiência técnica e deficiências sistêmicas formais, e que têm livre acesso investigativo e poderes de usar sanções necessárias como forma de impor suas decisões.

Reason (2006) propõe então um modelo pró-ativo de monitoramento dos erros (Figura 10), cujos dados puros utilizados podem ser obtidos em visitas a organização, tais como a não aplicação ou desvios das práticas seguras, manutenção ruim ou itens impróprios utilizados, falta de instruções ou treinos, sistema de trabalho pobre, entre outros, gerando os exemplos de não conformidade.

[2] também conhecido como LTI - *lost time injury*

Identificados os exemplos de não conformidade, o próximo passo do modelo é identificar as organizações e setores administrativos superiores que determinaram os exemplos de não conformidade locais. Para cada exemplo encontrado deve-se primeiramente gerar dois tipos de ação: uma para a organização regulada orientando-a a fazer o correto, e outro ao agente regulador para monitoramento e assistência à retificação e, caso não feito satisfatoriamente, impor algumas sanções.

Em seguida, uma escala de pontuação é utilizada, e de acordo com o impacto com que cada fator organizacional influencia o exemplo particular, uma pontuação é dada. Normalmente se usa uma escala de cinco pontos, onde zero é para os casos onde não se aplica e cinco para indicar influências crescentes. Do mesmo modo, para cada fator organizacional, ações devem ser sugeridas para serem executadas em nível organizacional, monitoradas e assistidas.

Esses valores são então agrupados para gerar um perfil dos fatores organizacionais, permitindo indicar – tanto para o regulador como a empresa regulada – quais os fatores (setores ou organizações superiores) que necessitam de reformas mais urgentes.

Sabendo-se que as condições latentes são dinâmicas e que uma empresa não resolve efetivamente todos os problemas de uma vez, a cada nova inspeção feita, velhos e novos exemplos de não conformidade são encontrados que, por sua vez, gerarão novos perfis dos fatores organizacionais. Uma sucessão desses perfis permitirá, tanto ao agente regulador como à empresa regulada, trilhar o progresso dos esforços empreendidos, formando parte de um grande processo cíclico de aprendizagem.

3.4 Construindo uma cultura de segurança, segundo Reason

Para Reason (2006), enquanto uma cultura nacional surge de um amplo compartilhamento de valores, a cultura organizacional é moldada principalmente pelo compartilhamento de práticas.

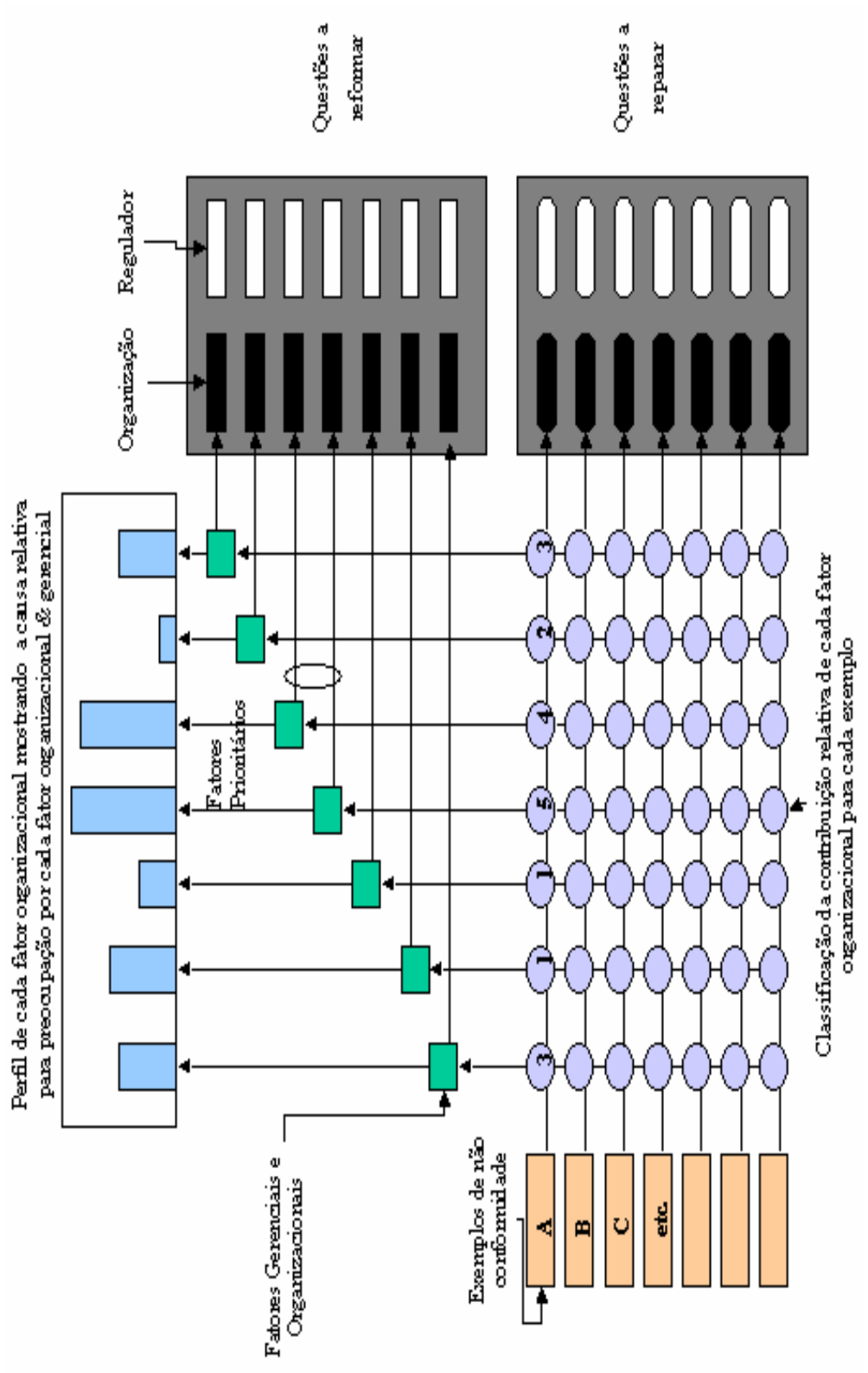
Portanto, uma cultura de segurança em uma organização deve ser um ideal, mesmo que seja difícil de ser alcançada. Deve-se basear em um respeito contínuo às várias entidades que podem penetrar e furar as defesas, do não esquecimento de

se ter medo, e de uma rede de informações consistente composta de informações coletadas, analisadas e disseminadas sobre incidentes e *near-misses*, assim como de checagens pro ativas regulares nos sinais vitais do sistema.

É necessário, portanto, criar uma **cultura de notificação** – um ambiente organizacional onde as pessoas estão preparadas para relatar seus erros e incidentes, dependente por sua vez, em como a organização manipula a culpa e punição. Para tal, uma **cultura de justiça** deve ser introduzida, em uma atmosfera de verdade nas quais as pessoas são encorajadas e recompensadas, em prover informações essenciais de relatos de segurança – mas que saibam também onde é o limiar do comportamento aceitável e inaceitável.

E que em caso de crise ou de um perigo eminente exista uma **cultura de flexibilidade (adaptabilidade)** como um fator essencial, dependente crucialmente de respeito – respeito por *skills*, experiências e habilidades dos colaboradores e, mais particularmente, os supervisores de primeira linha, lembrando que respeito deve ser merecido, e requer um investimento em treinamento forte por parte da organização. Finalmente, uma organização deve possuir uma **cultura de aprendizagem** – disposição e competência para desenhar as conclusões certas de seu sistema de informações de segurança, e o desejo de implementar as principais reformas quando sua necessidade for indicada.

Juntos, os quatro subcomponentes críticos identificados como parte de uma cultura de segurança interagem para criar uma cultura de informação a qual equivale, ao propósito do autor, com a “cultura de segurança”, quando se aplica ao campo de acidentes organizacionais.



Fonte: Reason, 2006
Figura 10 - Modelo de monitoramento das não conformidades

Reason (2006, p. 220) diz:

"... uma cultura de segurança, porém, é mais do que a soma dos seus componentes. Uma cultura é alguma coisa que uma organização 'é' mais do que ela 'tem'. Mas, para chegar a um estado satisfatório de 'é', primeiro tem de 'ter' os componentes essenciais. E esses já foram mostrados como se alcançam. O resto depende da química organizacional. O usar e o fazer levam ao pensar e acreditar. E se você está convencido de que sua organização tem uma boa cultura de segurança, está completamente enganado. Assim como um estado de graça, uma cultura de segurança é alguma coisa que você estará sempre buscando, mas nunca alcançando. O processo é mais importante do que o produto. A eficiência – e a recompensa – está na luta mais do que no retorno."