

MODOS DE FALHA DE UM SISTEMA DE GESTÃO DA SEGURANÇA

Fernando Moraes Ribeiro

RESUMO

O presente trabalho aborda as principais condições que podem levar um sistema de gestão da segurança a não atingir os objetivos pretendidos, denominadas modos de falha, bem como aspectos organizacionais que possibilitam a identificação e correção de tais condições.

1. INTRODUÇÃO

Antes que a expressão “Safety Management Systems” passasse a ter interpretações específicas em normas técnicas e regulamentos, um sistema de gestão da segurança poderia ser definido como “aquilo que alguém ou alguma organização faz para obter o que supõe ser a segurança”. A previsível variação daquilo que diferentes atores consideram necessário gerir, para obter o que os próprios supõem ser a segurança, permeia insucessos desde a explosão de um ônibus espacial até um acidente pessoal durante a execução de tarefas domésticas triviais.

Apesar dos tangíveis benefícios da uniformização global dos fundamentos para o controle dos riscos, possibilitando um maior grau de sucesso de indivíduos e organizações ao tentarem conduzir seus sistemas para um estado seguro, também é possível identificar cenários nos quais o ímpeto para evidenciar que se “tem” um sistema de gestão da segurança supera o de corrigir todas as condições que comprometem o controle dos riscos.

A eliminação ou mitigação dos modos de falha descritos a seguir aumenta a chance de sucesso de uma organização em relação aos próprios objetivos de segurança.

2. DESCRIÇÃO

Os principais modos de falha de um sistema de gestão da segurança, capazes de levar ao não atingimento dos objetivos de segurança pretendidos, são:

- Adoção de um paradigma incorreto de segurança;
- Segurança não gerida como um sistema;
- Foco em processos e metas não críticos para a segurança;
- Suposição de que a segurança possa ser eficazmente gerida em uma organização mal gerida; e
- Suposição de que a promoção da segurança possa compensar riscos mal controlados.

3. DISCUSSÃO

3.1 Adoção de um paradigma incorreto de segurança

Se o gestor de um sistema para obter qualquer coisa tiver uma compreensão incorreta do que seja essa coisa, o referido sistema está fadado ao insucesso, pois todos os recursos alocados ao sistema seriam polarizados em uma direção incorreta.

É admissível, no imaginário leigo, a percepção da segurança como a normalidade, ocasionalmente perturbada pelos acidentes, e restaurada por meio da adequada investigação. Tal paradigma talvez fosse aplicável a um bloco de chumbo flutuando no vácuo, mas, convenhamos, os domínios para os quais os fundamentos de sistemas de gestão da segurança foram uniformizados contém operações mais críticas e complexas.

Segundo Charles Perrow [1] o paradigma que mais contribui para o sucesso de um sistema de gestão da segurança é supor que, nas múltiplas interações dos elementos de sistemas complexos, em algum momento, alguma coisa dará errado. Em tais sistemas, portanto, a segurança é uma exceção penosamente construída pelo intelecto humano, em sucessivas vitórias contra as leis da natureza.

3.2 Segurança não gerida como um sistema

Segundo Charles Edwards Deming [2], um sistema é “uma rede de componentes interdependentes que trabalham em conjunto para tentar atingir um objetivo”; e “Sem objetivo, não existe sistema”.

A abordagem sistêmica ideal para a gestão da segurança seria que cada decisão que precede a alocação de recursos, quase sempre escassos, e sempre finitos, fosse tomada considerando não apenas informações isoladas sobre eventos ou resultados indesejados, e sim sobre o estado do sistema do qual emergiram tais informações.

Na ausência de uma abordagem sistêmica, cada problema é tratado como um novo problema, com causas inéditas e com recursos infinitos para as soluções. Ambas as premissas são falsas, e levarão ao insucesso do sistema.

3.3 Foco em processos e metas não críticos para a segurança

Segundo Bill Voss [3], “o jeito mais fácil de induzir pessoas a fazerem bobagem é medir seu desempenho em relação a objetivos insensatos”. Por vezes a profusão de modelos com pirâmides, icebergs e queijos furados na literatura de segurança influencia gestores a elegerem, como indicadores de segurança, métricas cuja variação não indica de fato em que grau os riscos estão controlados e quão confiáveis são tais controles.

O modelo mais sintético sobre o que é crítico saber, para um adequado monitoramento da segurança é: “segurança = proteção + confiança”, onde a proteção resulta dos controles, especificados por meio da gestão do risco, e a confiança resulta da verificação da eficácia destes, por meio da gestão da qualidade, de uma forma independente da ocorrência de eventos ou resultados indesejados.

Proteção sem confiança é uma aposta; confiança sem proteção é insanidade. Toda vez que algo dá errado, é importante saber se faltavam proteções adequadas, ou se proteções adequadas não tiveram o efeito desejado porque se degradaram à revelia do gestor do sistema. Essa é uma encruzilhada crítica em qualquer investigação, pois tomar o caminho errado levará ao desperdício de recursos escassos, contribuindo assim para insucessos recorrentes.

3.4 Suposição de que a segurança possa ser eficazmente gerida em uma organização mal gerida

Uma citação popular resume bem este modo de falha: “o rabo não vai abanar o cachorro”. Não é razoável supor que a gestão da segurança possa ser imune, tal qual uma bolha de excelência gerencial, a uma organização mal gerida.

Segundo Jack Welch [4] “pessoas demais — por vezes demais — intuitivamente não se expressam com franqueza”. (...) “Elas douram a pílula para tentar manter as aparências”; “isso é absolutamente danoso”;

e “Esqueçam a concorrência externa quando seu pior inimigo é a forma como vocês se comunicam internamente uns com os outros! ”.

Quão eficazes podem ser campanhas, por iniciativa do gestor da segurança, para tornar mais segura a cultura organizacional, em organizações onde informações críticas para outros objetivos da empresa, inclusive econômicos, são omitidas ou silenciadas para manter as aparências?

3.5 Suposição de que a promoção da segurança possa compensar riscos mal controlados

O modelo de Sistema de Gestão da Segurança Operacional utilizado pela Agência Nacional de Aviação Civil (ANAC) [5], em sintonia com o Safety Management Framework da Internacional Civil Aviation Organization (ICAO) [6] contém quatro componentes: 1- Política e Objetivos de Segurança; 2- Gerenciamento do risco; 3 - Garantia da segurança e 4- Promoção da segurança.

A promoção da segurança se refere à “capacitação, comunicação e outras ações para criar uma cultura de segurança positiva em todos os níveis da organização”. Toda vez que as recomendações em resposta a um evento adverso se limitam a “alertar”, “divulgar”, “treinar” ou ainda, o indefectível “conscientizar”, estaremos diante de mais uma tentativa de restaurar o nível desejado de controle dos riscos por meio de promoção da segurança.

Por mais relevante que seja a promoção da segurança, a existência no modelo de um componente exclusivo para o gerenciamento do risco evidencia que a promoção da segurança não supre a necessidade primordial de controlar riscos.

4. CONCLUSÃO

O conhecimento dos modos de falha de um sistema de gestão da segurança, bem como dos aspectos organizacionais que possibilitam identificá-los e corrigi-los, aumenta a chance de sucesso de uma organização em relação aos próprios objetivos de segurança.

5. REFERÊNCIAS:

- [1] PERROW, CHARLES, Normal accidents: living with high risk Technologies, Basic Books, US (1984);
- [2] DEMING, CHARLES EDWARDS, The New Economics for Industry, Government, Education, The MIT Press, UK, (1994);
- [3] VOSS, WILLIAM R., SMS Reconsidered, Flight Safety Foundation em <https://flightsafety.org/asw-article/sms-reconsidered/> (2012);
- [4] WELCH, JACK, Winning, Harper Business, US (2005);
- [5] Agência Nacional de Aviação Civil (ANAC), Os quatro componentes do SGSO, em <https://www.anac.gov.br/assuntos/paginas-tematicas/gerenciamento-da-seguranca-operacional/os-quatro-componentes-do-sgso> BR (2016);
- [6] International Civil Aviation Organization (ICAO), Doc 9859 NA/474 Safety Management Manual, em https://www.icao.int/safety/fsix/Library/DOC_9859_FULL_EN.pdf, CA (2009)