Cibersegurança e segurança dos processos

riscos diferentes, responsabilidades comuns

A perspectiva do conselho e da experiência operacional

Grandes crises raramente começam como uma surpresa total

Sinais

Desvios, incidentes e fragilidades já estavam presentes.

Barreiras

Controles existiam, mas eram frágeis, isolados ou não testados.

Governança

Informação não chegou, não foi compreendida ou não gerou ação.

O acidente ocorre quando a organização deixa o risco atravessar sucessivas barreiras.

A lógica de proteção é comum aos dois mundos

SEGURANÇA DE PROCESSOS		CIBERSEGURANÇA
Perigos e cenários de acidente	↔	Ameaças e cenários de interrupção
Barreiras preventivas e mitigadoras	↔	Proteção, detecção, resposta e recuperação
Integridade dos ativos e disciplina operacional	↔	Integridade de dados, sistemas e acessos
Planos e simulados de emergência	↔	Exercícios de crise e continuidade

Deepwater Horizon: barreiras técnicas e preparação falharam juntas

Explosão na plataforma em 2010: 11 trabalhadores morreram.

Antes

Decisões e sinais operacionais não foram integrados numa visão do risco total.

Durante

Barreiras de prevenção e controle do poço não impediram a escalada.

Depois

Indústria e governo não estavam preparados para conter um blowout em águas profundas.

Lição: resposta extraordinária não compensa a falta de preparação anterior.

Boeing 737 MAX: quando pressão, projeto e supervisão deixam de se equilibrar

Dois acidentes mataram 346 pessoas e levaram à suspensão mundial da aeronave.

Projeto

Premissas e dependências do sistema MCAS não foram tratadas com a robustez necessária.

Informação

Problemas relevantes não circularam com transparência suficiente.

Cultura e supervisão

Pressões organizacionais e falhas de certificação enfraqueceram a segurança.

Lição: cultura de segurança é o que permite interromper uma decisão tecnicamente perigosa.

Lojas Renner: contenção e recuperação preservaram a continuidade

O ataque de agosto de 2021 interrompeu canais digitais, mas as lojas físicas permaneceram abertas.

Contenção

A empresa acionou protocolos de segurança e isolou o impacto enquanto investigava o incidente.

Operação degradada

As lojas continuaram abertas, apesar da indisponibilidade temporária de alguns processos.

Recuperação

O site voltou em dois dias; o aplicativo e os sistemas prioritários foram restabelecidos em seguida.

Lição: resiliência exige prioridades claras e capacidade de operar durante a recuperação.

Colonial Pipeline: a falha em TI que paralisou o duto

O ransomware de 2021 levou à paralisação do maior sistema de dutos de combustíveis dos EUA.

Acesso

Uma conta de VPN legada usava apenas autenticação por senha, sem MFA.

Decisão operacional

A empresa interrompeu o transporte por não conseguir assegurar faturamento e integridade da operação.

Crise

Escassez, compras de pânico e pressão pública ampliaram rapidamente o impacto.

Lição: sem dados confiáveis, a empresa pode ter de interromper a operação.

C&M Software: uma credencial legítima permitiu transferências fraudulentas

O ataque de 2025 atingiu uma provedora que conectava instituições financeiras ao Banco Central.

Acesso interno

Segundo a investigação policial, um funcionário teria vendido suas credenciais a criminosos.

Autoridade excessiva

O acesso legítimo possibilitou comandos financeiros de alto valor por meio da infraestrutura da provedora.

Contenção sistêmica

O Banco Central desconectou a C&M e impôs condições para a retomada das operações.

Lição: uma credencial válida também precisa de limites, dupla aprovação e monitoramento.

Wells Fargo: metas sem controles transformaram estratégia em risco

O Federal Reserve restringiu o crescimento do banco até a melhoria da governança e dos controles.

Estratégia

O crescimento foi priorizado sem gestão adequada de todos os riscos relevantes.

Escalonamento

Falhas de compliance graves não chegaram ao conselho de forma efetiva.

Supervisão

O regulador exigiu mudanças no conselho, controles e gestão de riscos.

Lição: incentivos e metas também são componentes do sistema de controle.

Riscos diferentes atravessam as mesmas fragilidades de governança

01	Sinais dispersos	Incidentes, quase-acidentes e exceções não formam uma visão integrada.
02	Barreiras frágeis	Controles existem no papel, mas não têm desempenho demonstrado.
03	Pressão organizacional	Prazo, custo ou crescimento silenciam alertas e normalizam desvios.
04	Escalonamento tardio	A liderança conhece o problema quando as opções já são limitadas.

A matriz precisa ser viva, conectada ao negócio e atualizada por incidentes

1. Cenários

Ataques
Falhas operacionais
Clima extremo
Terceiros

→

2. Funções críticas

Segurança
Operação
Dados e serviços
Caixa e reputação

→

3. Barreiras

Prevenir
Detectar
Conter
Recuperar

→

4. Risco residual

Tolerância
Planos alternativos
Decisões
Comunicação

Entradas obrigatórias: incidentes internos, eventos externos, mudanças tecnológicas e novos riscos climáticos.

Indicadores preventivos mostram a exposição antes que a perda aconteça

PREVENTIVOS

- Vulnerabilidades críticas fora do prazo
- Barreiras testadas e falhas encontradas
- Acessos privilegiados e exceções abertas
- Simulados, terceiros críticos e cobertura

REATIVOS

- Incidentes por severidade e impacto
- Tempo de detecção, contenção e recuperação
- Perdas operacionais, financeiras e de dados
- Recorrência e eficácia das ações corretivas

Um painel equilibrado evita que o conselho descubra o risco apenas pelo incidente.

A crise precisa de uma governança definida antes do primeiro alerta

01	Autoridade	Quem declara a crise, interrompe operações e mobiliza recursos?
02	Decisão	Quais dados mínimos, tolerâncias e prioridades orientam escolhas?
03	Integração	Tecnologia, operação, jurídico, pessoas e comunicação atuam juntos?
04	Aprendizado	Simulados e incidentes alteram planos, barreiras e responsabilidades?

O conselho não opera a crise — assegura a preparação

01	Direcionar	Conectar cibersegurança, estratégia, segurança e continuidade.
02	Definir tolerâncias	Traduzir apetite a risco em limites operacionais compreensíveis.
03	Supervisionar	Desafiar tendências, exceções, barreiras e planos de tratamento.
04	Exercitar decisões	Participar de simulações realistas com gestão e terceiros críticos.

Riscos diferentes exigem a mesma maturidade de governança.

Identificar não basta.

É preciso monitorar, testar barreiras, aprender com incidentes e decidir antes que a emergência retire nossas opções.

Segurança é uma capacidade organizacional — não apenas técnica.