

EDIÇÃO Nº 001 | OUTUBRO DE 2026

Quando a prevenção falha: sua empresa está preparada para continuar operando?

Três acontecimentos recentes e suas implicações para a segurança, a governança e a continuidade dos negócios.



■ VISÃO EXECUTIVA

Segurança não termina na prevenção.

Três acontecimentos recentes, em contextos distintos, reforçam a importância de preparar organizações para situações em que seus mecanismos preventivos não sejam suficientes.

OS TRÊS ACONTECIMENTOS

01**G7**

Ministros de finanças e presidentes de bancos centrais acordam exercícios que simulam ciberataques potencializados por inteligência artificial.

Reuters, out. 2026 · p. 3

02**Banco da Inglaterra**

Autoridade defende opções de recuperação para serviços essenciais quando o ambiente tecnológico principal estiver comprometido.

Reuters; BoE, out. 2026 · p. 5

03**Hospital Sírio-Libanês**

Instituição comunica possível acesso não autorizado a um sistema interno de relatórios ligado a projetos sociais.

Comunicado, out. 2026 · p. 7

O CICLO DA RESILIÊNCIA

FOCO DESTE BRIEF: QUANDO A PREVENÇÃO NÃO É SUFICIENTE



MENSAGEM PRINCIPAL

A maturidade de uma organização também deve ser avaliada por sua capacidade de **identificar, responder, recuperar operações e preservar a confiança** de clientes, parceiros e demais partes interessadas.



■ CASO 1 · G7 E INTELIGÊNCIA ARTIFICIAL

Quando a resposta a incidentes se torna uma preocupação sistêmica.

O FATO

Reuters, 16 out. 2026 [1]

Em 15 de outubro de 2026, a ministra das Finanças do Japão, Satsuki Katayama, informou que os ministros de finanças e presidentes de bancos centrais do G7, reunidos em Bangkok, aprovaram a realização de **exercícios de mesa sobre IA de fronteira**. As simulações, desenvolvidas pelas autoridades financeiras do grupo, testarão a resposta a ciberataques potencializados por IA.¹

De acordo com a reportagem, os exercícios poderão incluir instituições financeiras privadas, conforme o cenário, e os resultados servirão para avaliar protocolos e revisar manuais existentes. O anúncio ocorreu após alerta do FMI de que um ataque com uso de IA contra um serviço crítico de uma instituição financeira poderia abalar a confiança no sistema.¹



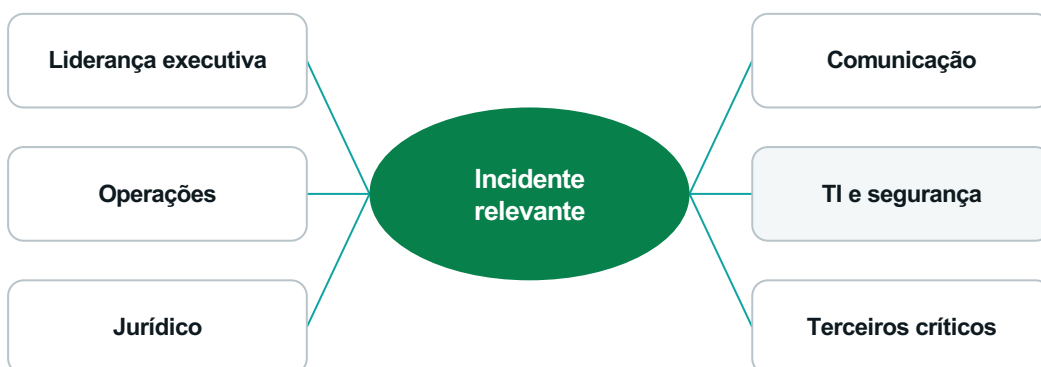
■ CASO 1 · G7 E INTELIGÊNCIA ARTIFICIAL · CONTINUAÇÃO

ANÁLISE SHIELD

Interpretação da Shield Consulting

Um incidente que interrompe serviços críticos raramente permanece restrito à área técnica: seus efeitos alcançam clientes, contrapartes e reguladores e exigem decisões rápidas e consistentes. Por isso, a coordenação entre instituições e autoridades é parte da própria resposta.

Um plano de resposta a incidentes não pode depender exclusivamente da equipe de TI ou de segurança da informação. Incidentes relevantes exigem decisões coordenadas envolvendo operações, jurídico, comunicação, liderança executiva e terceiros críticos.



Resposta coordenada: a equipe técnica é uma das partes envolvidas, não a única.

RECOMENDAÇÕES

O que avaliar e testar

01

Realizar exercícios de mesa envolvendo diferentes áreas

Com cenários que incluam indisponibilidade de serviços críticos e participação de fornecedores.

02

Definir autoridades de decisão e critérios de escalonamento

Quem declara a crise, quem aprova a comunicação externa e quando acionar autoridades.

03

Validar canais alternativos de comunicação

Que funcionem mesmo com e-mail, diretório corporativo ou ferramentas de colaboração indisponíveis.

04

Registrar decisões e oportunidades de melhoria

Durante o exercício e o incidente, com responsáveis e prazos para cada ação.



■ CASO 2 · BANCO DA INGLATERRA

Ter backup não significa estar preparado para recuperar operações.

O FATO

Reuters, 15 out. 2026 [2]; Bank of England, 9 out. 2026 [3]

Em 15 de outubro de 2026, Sarah Breeden, vice-presidente do Banco da Inglaterra, afirmou que os bancos não podem mais presumir que suas defesas são impenetráveis diante de ataques potencializados por IA. Segundo a Reuters, o banco central trabalha com as instituições em opções de **recuperação “bare metal”**: sistemas independentes da infraestrutura principal, acionáveis quando os sistemas primários estão comprometidos.²

Uma semana antes, o CMORG, grupo de resiliência operacional presidido pelo Banco da Inglaterra e pela UK Finance, concluiu o **SIMEX26**, exercício setorial que simulou uma interrupção global de serviços em nuvem com as 38 maiores instituições e infraestruturas de mercado do Reino Unido.³

TRÊS CONCEITOS

Escopos diferentes, perguntas diferentes

Backup

Cópias de dados e configurações preservadas em local separado.

Os dados existem e estão íntegros?

Recuperação de desastres

Capacidade de restaurar sistemas e infraestrutura em prazo definido.

Conseguimos reconstruir o ambiente tecnológico?

Continuidade de negócios

Capacidade de manter ou retomar processos críticos, inclusive por meios alternativos.

O negócio continua entregando o essencial?



Imagem gerada por IA

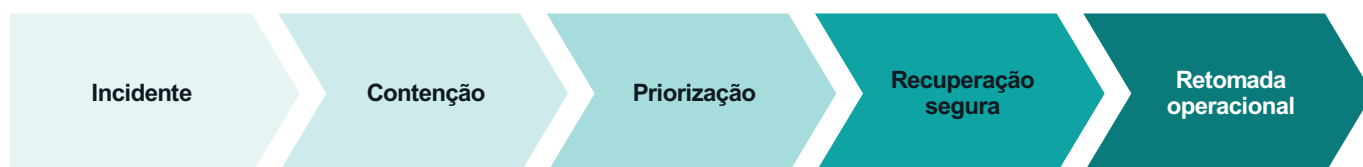


■ CASO 2 · BANCO DA INGLATERRA · CONTINUAÇÃO

ANÁLISE SHIELD

Interpretação da Shield Consulting

A existência de cópias de segurança não comprova, isoladamente, a capacidade de recuperar processos e serviços críticos. A organização precisa compreender dependências, prioridades, tempos de recuperação e condições mínimas para uma retomada segura.



Da ocorrência à retomada: recuperar com segurança exige conter a ameaça e priorizar o que retorna primeiro.

RECOMENDAÇÕES

O que avaliar e testar

01 Validar RTO e RPO com as áreas de negócio

Tempos e perdas toleráveis devem refletir o impacto no negócio, não só a capacidade técnica.

02 Testar restaurações em ambientes isolados

Para confirmar a integridade e evitar reintroduzir a ameaça no ambiente recuperado.

03 Considerar o comprometimento de credenciais administrativas

Cópias e consoles acessíveis pelas mesmas contas podem ser afetados pelo mesmo ataque.

04 Exercitar procedimentos alternativos de operação

Formas manuais ou degradadas de manter o essencial enquanto a tecnologia é restaurada.

05 Verificar dependências de provedores externos

Nuvem, software e serviços terceirizados com papel na recuperação e seus compromissos contratuais.



■ CASO 3 · HOSPITAL SÍRIO-LIBANÊS

O risco de privacidade também existe fora dos sistemas principais.

**O FATO**

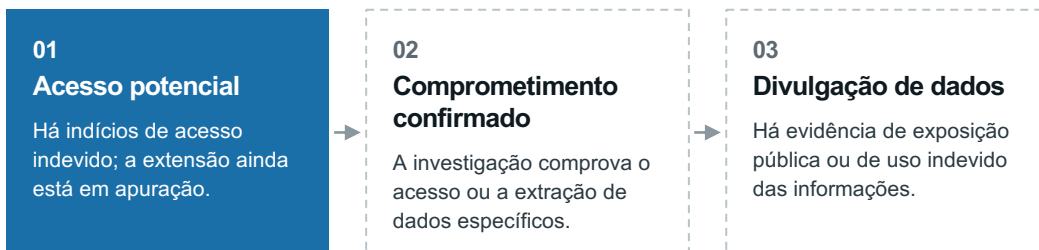
Comunicado institucional, out. 2026 [4]

Em comunicado publicado em outubro de 2026, a Sociedade Beneficente de Senhoras Hospital Sírio-Libanês informou ter identificado, em 21 de setembro, um **possível acesso não autorizado** a um sistema interno de relatórios que reúne parte das informações de pessoas ligadas a alguns de seus projetos sociais. O caso foi reportado à ANPD, em formato preliminar, e à Polícia Federal.⁴

Segundo o hospital, a apuração indica a possibilidade de acesso a dados cadastrais e de atendimento, incluindo dados sensíveis, sem evidências, até o momento, de divulgação pública ou uso indevido. Os atendimentos seguem sem interrupção.⁴

**CASO 3 · HOSPITAL SÍRIO-LIBANÊS · CONTINUAÇÃO****TRÊS SITUAÇÕES**

Cada uma exige evidências próprias



Situação descrita pelo hospital até a data desta edição. O hospital não confirmou vazamento ou uso indevido dos dados.

ANÁLISE SHIELD

Interpretação da Shield Consulting

Aplicações secundárias, integrações, plataformas departamentais e fornecedores também integram a superfície de risco da organização. A governança de privacidade precisa abranger todos os ambientes que tratam dados pessoais.

As medidas descritas no comunicado (isolamento, preservação de registros, verificação das cópias de segurança e redefinição de credenciais) ilustram uma resposta estruturada. Distinguir o potencial, o confirmado e o divulgado orienta contenção, notificação e comunicação.

RECOMENDAÇÕES

O que avaliar e testar

01 Manter inventário de aplicações e tratamentos de dados

Inclusive sistemas de relatórios, planilhas, integrações e plataformas de projetos.

02 Identificar responsáveis pelos sistemas e informações

Cada ambiente com dados pessoais precisa de um responsável de negócio e um técnico.

03 Revisar acessos e integrações

Contas de serviço, perfis privilegiados e conexões com terceiros, de forma periódica.

04 Classificar dados pessoais e sensíveis

Para dimensionar com rapidez os impactos e os titulares potencialmente afetados.

05 Validar procedimentos de avaliação e comunicação de incidentes

Critérios, prazos e responsáveis alinhados à LGPD e às orientações da ANPD.



■ ANÁLISE INTEGRADA

Três acontecimentos. Uma mesma questão de governança.

Vistos em conjunto, os casos levam às mesmas perguntas de governança. A matriz relaciona cada dimensão aos acontecimentos em que ela aparece com mais clareza.

DIMENSÃO	QUESTÃO PRINCIPAL	G7	BoE	Sírio-Libanês
Resposta	Quem decide quando um incidente ultrapassa a capacidade técnica?	●	○	●
Continuidade	Quais processos precisam continuar operando?	○	●	○
Recuperação	Como restauramos serviços em ambientes comprometidos?	○	●	○
Privacidade	Sabemos quais dados e titulares podem ser afetados?	—	—	●
Confiança	Como comunicamos e preservamos relações com partes interessadas?	●	○	●

● relação direta ○ relação indireta — sem relação evidente nas fontes Avaliação da Shield Consulting com base nas fontes citadas.

CONCLUSÃO DA ANÁLISE

Ferramentas isoladas não substituem **governança, responsabilidades claras e capacidades testadas.**

Tecnologia de proteção é necessária. Mas a resposta a um incidente relevante depende de quem decide, do que precisa continuar operando e de quanto a organização já testou essas respostas.

Governança

Quem decide, com que autoridade e com base em quais critérios.

Responsabilidades claras

Donos de processos, sistemas, dados e fornecedores definidos antes do incidente.

Capacidades testadas

Exercícios e testes que mostram o que funciona e o que precisa melhorar.



■ CINCO PERGUNTAS PARA A LIDERANÇA

Sua organização está realmente preparada?

Perguntas para orientar a próxima reunião de diretoria ou de comitê de riscos. Respostas vagas ou divergentes entre as áreas indicam por onde começar.

01 Quem tem autoridade para declarar um incidente crítico e coordenar as decisões?

EVIDÊNCIA DE PREPARO Matriz de decisão aprovada, com substitutos definidos e conhecidos.

02 Quais serviços precisam ser recuperados primeiro e em quanto tempo?

EVIDÊNCIA DE PREPARO Serviços priorizados, com RTO e RPO acordados com as áreas de negócio.

03 Já testamos a recuperação quando o ambiente principal está comprometido?

EVIDÊNCIA DE PREPARO Teste de restauração em ambiente isolado, com resultados documentados.

04 Conseguimos identificar rapidamente os dados pessoais potencialmente afetados?

EVIDÊNCIA DE PREPARO Inventário atualizado de sistemas, dados tratados e responsáveis.

05 Quando foi realizado o último exercício conjunto entre segurança, operações, jurídico e comunicação?

EVIDÊNCIA DE PREPARO Exercício recente, com plano de melhorias acompanhado pela liderança.

Como usar: registre as respostas, os responsáveis e as evidências disponíveis. As lacunas identificadas alimentam o plano de 30, 60 e 90 dias da página seguinte.



RECOMENDAÇÕES DA SHIELD CONSULTING

Da conscientização à capacidade comprovada.

Um roteiro em três horizontes para transformar as lições destes casos em capacidades verificáveis pela liderança.

PRÓXIMOS 30 DIAS Organizar	PRÓXIMOS 60 DIAS Testar	PRÓXIMOS 90 DIAS Consolidar
OBJETIVO Clareza de papéis, prioridades e ativos.	OBJETIVO Evidência prática do que funciona.	OBJETIVO Melhorias incorporadas à rotina.
- Revisar responsáveis e fluxos de escalonamento - Identificar serviços e dependências críticas - Verificar inventários de aplicações e dados	- Realizar exercício de resposta a incidentes - Testar a recuperação de serviços prioritários - Identificar lacunas de coordenação	- Implementar melhorias prioritárias - Atualizar procedimentos e responsabilidades - Estabelecer indicadores de prontidão - Apresentar resultados à liderança
RESULTADO ESPERADO Mapa atualizado de decisões, serviços críticos e dados.	RESULTADO ESPERADO Capacidades testadas e lacunas documentadas.	RESULTADO ESPERADO Prontidão mensurada e reportada à liderança.

EXEMPLOS DE INDICADORES DE PRONTIDÃO

Serviços críticos com RTO e RPO validados

Proporção dos serviços priorizados com metas acordadas com o negócio.

Recuperação testada

Serviços prioritários restaurados com sucesso em teste isolado no período.

Exercícios conjuntos

Tempo desde o último exercício com segurança, operações, jurídico e comunicação.

Cobertura do inventário

Sistemas com dados pessoais inventariados e com responsável definido.

Nota: os prazos são uma proposta de priorização, não uma exigência regulatória universal. Devem ser ajustados ao porte, ao setor e às obrigações de cada organização.

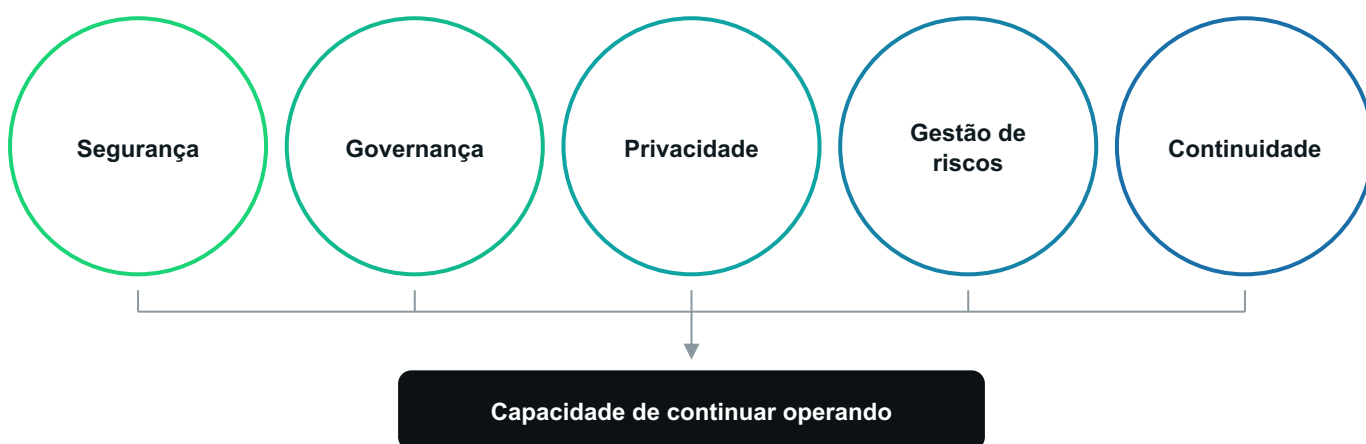


■ CONCLUSÃO

A prevenção reduz riscos. A resiliência preserva o negócio.

Os três acontecimentos tratados neste brief vêm de contextos diferentes: autoridades financeiras internacionais, um banco central e uma instituição de saúde. Em comum, mostram que a preparação de uma organização também se mede pelo que acontece depois que um controle falha.

Responder com coordenação, recuperar com segurança, saber quais dados estão em jogo e comunicar com precisão são capacidades que dependem de decisões tomadas antes do incidente. Por isso, **segurança, governança, privacidade, gestão de riscos e continuidade precisam funcionar como um sistema único**, e não como iniciativas paralelas.



O QUE OS TRÊS CASOS MOSTRAM

CASO 1 · G7

Resposta é uma decisão coordenada

Incidentes relevantes exigem decisões que envolvem operações, jurídico, comunicação, liderança executiva e terceiros críticos.

CASO 2 · BANCO DA INGLATERRA

Backup não comprova recuperação

É preciso conhecer dependências, prioridades e tempos de recuperação, e testar a retomada com o ambiente principal comprometido.

CASO 3 · SÍRIO-LIBANÊS

Privacidade vai além dos sistemas principais

Aplicações secundárias, integrações e fornecedores também tratam dados pessoais e precisam estar sob a mesma governança.

Em comum, os três casos indicam que a preparação precisa ser comprovada antes do incidente: com responsáveis definidos, prioridades acordadas e exercícios realizados.



■ SOBRE A SHIELD CONSULTING

Segurança, governança e continuidade, da estratégia à execução.

A Shield Consulting é uma consultoria especializada em segurança da informação, governança, privacidade, gestão de riscos e continuidade de negócios.

Seu trabalho conecta estratégia, governança e execução: da avaliação de maturidade ao desenho de responsabilidades, processos e planos de continuidade.

ATUAÇÃO INTEGRADA

- 01 Segurança da informação e cibersegurança
- 02 Governança, riscos e conformidade
- 03 Privacidade e proteção de dados
- 04 Continuidade e resiliência operacional
- 05 Gestão empresarial e melhoria de processos

AVALIAÇÃO DE MATURIDADE · GOREADY

Sua organização está realmente preparada?

Descubra como sua empresa está posicionada em dimensões essenciais de gestão, governança e resiliência.

Faça sua avaliação de maturidade com o GoReady.

goready.shield-consulting.com

Site institucional: shield-consulting.com



Aponte a câmera para acessar o GoReady



■ FONTES E REFERÊNCIAS

Fontes e referências

Fontes consultadas em 19 de outubro de 2026. Os números entre colchetes correspondem às citações nas páginas dos casos.

G7

Outubro de 2026

[1] Reuters. “G7 to launch exercises to guard against AI cyber attacks”

Reportagem, 16 out. 2026 · Citada na página 3

<https://www.reuters.com/world/asia-pacific/g7-launch-exercises-guard-against-ai-cyber-attacks-2026-10-16/>

BANCO DA INGLATERRA

Outubro de 2026

[2] Reuters. “Banks need ‘bare metal’ recovery in face of AI risks, says BoE’s Breeden”

Reportagem, 15 out. 2026 · Citada na página 5

<https://www.reuters.com/legal/litigation/banks-need-bare-metal-recovery-face-ai-risks-says-boes-breeden-2026-10-15/>

[3] Bank of England. “CMORG holds sector-wide cloud outage simulation exercise” (SIMEX26)

Comunicado, 9 out. 2026 · Citado na página 5

<https://www.bankofengland.co.uk/news/2026/october/cmorg-holds-sector-wide-cloud-outage-simulation-exercise>

HOSPITAL SÍRIO-LIBANÊS

Outubro de 2026

[4] Hospital Sírio-Libanês. “Informações sobre o Incidente de Segurança da Informação” (Perguntas Frequentes)

Comunicado institucional, out. 2026 · Citado na página 7

<https://hospitalsiriolibanes.org.br/faq>

[5] UOL Notícias. Reportagem sobre o possível acesso não autorizado a sistema interno do hospital

Reportagem, 16 out. 2026 · Referência complementar (ver nota)

<https://noticias.uol.com.br/cotidiano/ultimas-noticias/2026/10/16/hospital-sirio-libanes-possivel-acesso-nao-autorizado-sistema-interno.ghnm>

NOTA METODOLÓGICA

As matérias da Reuters [1] e [2] foram conferidas por meio de republicações do despacho original da agência. A reportagem do UOL [5] não pôde ser acessada para conferência e é listada apenas como referência complementar; seu conteúdo não foi utilizado nesta análise.

AVISO

As notícias e informações públicas reunidas nesta publicação são de responsabilidade exclusiva das fontes primárias. A Shield Consulting atua na curadoria e na análise e não se responsabiliza pela veracidade ou pela atualização dos fatos divulgados pelas fontes originais. As análises e recomendações têm caráter informativo e não substituem uma avaliação específica de cada organização.

IMAGENS

As imagens desta publicação foram geradas com auxílio de inteligência artificial e possuem caráter exclusivamente ilustrativo. Não representam registros fotográficos dos acontecimentos, pessoas ou instalações mencionadas.