GRCForce

Estrutura de governação da resposta a incidentes: Lista de preparação e guia de simulação

8 de julho de 2026

grcforce.com/pt/#contact

Practical governance, risk and compliance guidance for European organisations.

Lista de preparação e guia de simulação

Um guia prático para resposta a incidentes, comando de crise e preparação da notificação regulamentar.

Utilize este guia antes do próximo exercício, revisão regulamentar ou conversa de garantia de resiliência. Ajuda CISOs, responsáveis de GRC, líderes de incidentes e direção a testar se a governação acima da resposta técnica resistirá sob pressão.

Conteúdo

- Matriz de governação da resposta a incidentes
- Lista de preparação
- Referência de notificação regulamentar
- Classificação de gravidade
- Guia de simulação priorizado
- Cinco perguntas para a primeira hora
- Uma ação para esta semana
- Próximo passo

Um modelo prático para resposta, comando de crise e notificação

Numa crise, as organizações descem ao nível da sua preparação.

A maioria possui um plano; poucas testaram se a governação funciona realmente: autoridade de comando, comunicação externa, decisões entre contenção e continuidade e cumprimento dos prazos regulamentares.

Utilize o guia para testar o realismo operacional, preparar exercícios NIS2 ou DORA, melhorar o comando de crise, planear simulações, rever ações após incidentes e apoiar conversas com conselhos, clientes ou reguladores.

O objetivo não é criar mais documentação, mas saber se o modelo resistirá quando a pressão for real.

Matriz de governação

Camada	Preparar	Responder	Aprender	Responsável pelas evidências	Estado
1. Comando	Funções e substitutos nomeados; escalamento documentado	Líder ativo, cadência clara e direitos de decisão compreendidos	Lacunas revistas após exercícios e incidentes	Comandante do incidente / CISO	Verde / Âmbar / Vermelho
2. Decisões	Limiares e decisores substitutos definidos	Decisões críticas tomadas no nível certo sem atraso	Bloqueios analisados e corrigidos	Comandante / Direção executiva	Verde / Âmbar / Vermelho
3. Comunicações	Modelos internos, para clientes, media e colaboradores preparados	Mensagens aprovadas e emitidas na sequência e canal certos	Atrasos e confusão utilizados para melhoria	Comunicação / Jurídico	Verde / Âmbar / Vermelho
4. Notificação	Obrigações, prazos, contactos e modelos documentados	Cadeia de aprovação funciona sob pressão	Falhas e atrasos geram melhoria	Conformidade / Jurídico	Verde / Âmbar / Vermelho
5. Aprendizagem	Método e responsabilidade de revisão acordados	Evidências recolhidas durante o evento	Ações acompanhadas até ao encerramento	GRC / Risco	Verde / Âmbar / Vermelho

Pontuação rápida

- Verde: documentado, atribuído, atualizado e testado
- Âmbar: existe, mas está desatualizado, incompleto ou pouco claro sob pressão
- Vermelho: ausente, sem responsável ou suscetível de falhar

Mais de duas camadas vermelhas exigem correção antes do próximo exercício.

Lista de preparação

1. A autoridade de comando está atribuída

- Uma pessoa nomeada detém autoridade operacional
- Uma pessoa sénior assume a crise ao nível executivo
- O escalamento está documentado e compreendido
- Existem substitutos para todas as funções críticas
- A estrutura foi testada nos últimos 12 meses

2. Os direitos de decisão são explícitos

- A equipa técnica conhece as aprovações que pode dar sem escalamento
- A gestão conhece as decisões que exigem direção executiva
- Os limiares de notificação ao conselho estão documentados
- Pagamento, encerramento e comunicação têm vias acordadas
- Nenhuma decisão crítica depende de uma só pessoa indisponível

3. As comunicações estão preparadas

- Modelos internos acessíveis
- Declarações provisórias para clientes e parceiros
- Canais alternativos disponíveis
- Texto para media quando aplicável
- Cadeia de aprovação testada

4. A notificação regulamentar está operacionalmente preparada

- Obrigações NIS2, DORA, RGPD ou setoriais documentadas
- Contactos e canais atualizados
- Modelos iniciais, intermédios e finais disponíveis
- Vias de aprovação acordadas e testadas
- Jurídico, conformidade, comunicação e direção conhecem as funções

5. As relações externas estão preparadas

- Suporte externo de resposta ou forense confirmado
- Apoio jurídico experiente identificado
- Processo e contactos de seguro cibernético conhecidos
- Apoio de comunicação de crise identificado
- Vias de escalamento de fornecedores e cloud documentadas

Falha comum: terceiros críticos são contactados por primeira vez durante o incidente.

6. O modelo reflete a realidade operacional

- Plano revisto nos últimos 12 meses
- Sistemas, fornecedores e equipas atuais refletidos

- Serviços prioritários definidos
- Pressupostos essenciais testados
- Cenários de ransomware, disponibilidade e pressão de notificação abrangidos

Falha comum: o plano ainda descreve a organização como era há duas reorganizações.

Referência de notificação regulamentar

Referencial	Prazo inicial	Destinatário	Gatilho
NIS2 (UE)	24 h — alerta precoce	CSIRT nacional / autoridade competente	Incidente significativo
NIS2 (UE)	72 h — notificação	CSIRT nacional / autoridade competente	Incidente significativo
Artigo 33.º RGPD	72 h	Autoridade de controlo	Violação com risco para pessoas
DORA — setor financeiro UE	No prazo de 4 horas após a classificação como grave e, no máximo, 24 horas após a deteção — inicial	Autoridade competente	Incidente grave de TIC
DORA — setor financeiro UE	72 h — intermédia	Autoridade competente	Incidente grave de TIC
UK GDPR	72 h	ICO	Violação com risco para pessoas
Setorial	Variável	Regulador setorial	Evento significativo definido pelo setor

Ação: confirme as obrigações aplicáveis e documente contactos, canais e aprovação.

Classificação de gravidade

Nível	Descrição	Exemplos	Resposta
Nível 1 — Evento	Atividade suspeita sem impacto confirmado	Acesso invulgar, tentativas falhadas, tráfego anómalo	Investigação SOC, sem escalamento
Nível 2 — Incidente	Falha de controlo confirmada, impacto limitado e contido	Malware isolado, credencial comprometida sem acesso a dados	Ativar equipa e informar gestão
Nível 3 — Significativo	Impacto material em sistemas, serviços ou dados	Ransomware, exfiltração, indisponibilidade prolongada	Ativar comando de crise e avaliação regulamentar
Nível 4 — Crise	Serviços críticos afetados e impacto grave	Ransomware generalizado, grande violação, falha multissistema	Comando completo, notificação e liderança executiva

Os limiares de notificação regulamentar correspondem geralmente aos níveis 3 ou 4. Confirme os limiares com as equipas jurídica e de conformidade.

Guia de simulação priorizado

Prioridade	Cenário	O que testa	Razão
Alta	Ransomware com backups cifrados	Recuperação sem disponibilidade de TI	Expõe falsos pressupostos
Alta	Exfiltração sob pressão de notificação	Cadeia de aprovação e modelos	Exposição regulamentar e reputacional
Alta	Falha de terceiro ou cloud	Operação degradada de serviços críticos	Dependência crescente
Média	Ameaça interna e abuso de privilégios	Coordenação entre registos, RH, jurídico e segurança	Difícil deteção

Prioridade	Cenário	O que testa	Razão
Média	Falha cibernética e da cadeia de abastecimento	Gestão simultânea de crises	Limites de resiliência
Média	Falha de comunicação executiva	Governação sob pressão pública	Elevado risco reputacional
Baixa	Pedido de pagamento de ransomware	Quadro de decisão do conselho	Elevada pressão
Baixa	Auditoria durante incidente	Exigências paralelas	Governação intensiva
Baixa	Phishing na equipa financeira	Resposta conjunta	Coordenação negócio-cibersegurança
Baixa	Falha física em local sensível	Integração física e cibernética	Instalações ou dados sensíveis

Priorize de acordo com o seu modelo de ameaças: um fabricante deve testar a segurança física; um fornecedor SaaS deve priorizar cenários de falha na cloud.

Cinco perguntas para a primeira hora

1. O que aconteceu? O que está confirmado e o que é pressuposto?
2. Está contido? A ameaça continua ativa ou a propagar-se?
3. Quem precisa de saber? Que partes devem ser informadas agora?
4. Qual é o serviço prioritário? Que serviço crítico proteger primeiro?
5. Que prazos estão a decorrer? Que prazos regulamentares, contratuais ou comerciais já começaram?

Uma ação para esta semana

Teste a cadeia de aprovação de notificação para um incidente numa sexta-feira às 16h00: decisor disponível, substituto, modelo preparado e localização acessível sem a rede corporativa.

Próximo passo

A GRCForce pode realizar uma Revisão de Preparação da Resposta a Incidentes cobrindo comando, notificação, comunicação, simulação e governação pós-exercício.

Comece em https://grcforce.com/pt/#contact.