

Checklist Executivo: Resposta a Incidentes

Ações prioritárias e decisões críticas para as primeiras 12 a 72 horas após um ataque

EMPRESA	[Nome da Empresa / Organização]	DATA / HORA	____/____/____ às ____:____
LÍDER DE CRISE	[Nome do Responsável]	SUPERVISOR TI	[Responsável Técnico TI / CISO]

1. CONTENÇÃO E ISOLAMENTO IMEDIATO (0 - 4 HORAS)

- ☐ Isolar imediatamente os sistemas afetados e desconectar segmentos de rede comprometidos.
- ☐ Ativar canais de comunicação seguros fora do ambiente possivelmente comprometido.
- ☐ Preservar evidências digitais e logs antes de reiniciar ou desligar servidores afetados.
- ☐ Bloquear credenciais administrativas e congelar acessos de integração de terceiros.
- ☐ Verificar e proteger os repositórios de backup garantindo imutabilidade e isolamento.

2. GOVERNANÇA E COMITÊ DE CRISE (4 - 12 HORAS)

- ☐ Convocar o Comitê Executivo de Crise (TI, Diretoria, Jurídico, Comunicação e Operações).
- ☐ Calcular a taxa de impacto financeiro por hora de paralisação e definir prioridades operacionais.
- ☐ Ativar procedimentos manuais contingenciais para os processos essenciais de negócio.
- ☐ Notificar o seguro cibernético e acionar a assessoria jurídica especializada em LGPD/ANPD.
- ☐ Alinhar notas de comunicação interna para equipes e definir porta-voz oficial.

3. AMBIENTE LIMPO E RECUPERAÇÃO (12 - 48 HORAS)

- ☐ Subir um ambiente de recuperação isolado (Ambiente Limpo) para restauração segura.
- ☐ Mapear dependências críticas (Identidade, DNS, Nuvem) antes de reativar cada aplicação.
- ☐ Validar integridade dos backups antes da restauração para evitar contaminação por malware.
- ☐ Restaurar em ordem sequencial: infraestrutura base -> dados cruciais -> aplicações de negócio.

4. ESTABILIZAÇÃO E CONFORMIDADE (48 - 72 HORAS)

- ☐ Avaliar o vazamento de dados pessoais e documentar relatórios de impacto para a ANPD/Titulares.
- ☐ Homologar a segurança do ambiente restaurado antes de liberar o tráfego dos usuários.
- ☐ Revisar e atualizar o Plano de Resposta a Incidentes com base nas lições aprendidas.