Linha do tempo para a restauração da operação (Empresa S.A.)

Contexto: após o incidente de vazamento de fotos pessoais de clientes, a resposta inicial mitigou o impacto. Abaixo está a timeline (momento 0 = início do incidente) para voltar ao funcionamento normal.

0–2h após o incidente	• Ativar o Comitê de Crise e a gestão de incidentes, definindo líder, canal oficial e cadência de updates. • Confirmar o escopo inicial do vazamento (quais sistemas/dados) e bloquear imediatamente novas saídas de dados (regras de rede/DLP). • Preservar evidências (logs, imagens, snapshots) e registrar linha do tempo de ações para auditoria e conformidade (LGPD).
2–6h	• Conter o vetor de ataque: isolar ativos afetados, aplicar bloqueios/patch emergencial e revisar acessos privilegiados. • Rotacionar credenciais e segredos críticos (tokens, chaves, senhas) e forçar reset para contas de maior risco. • Iniciar comunicação interna com orientações claras (o que pode/não pode ser feito) e “single source of truth”.
6–12h	• Executar varredura de comprometimento (EDR/AV/IOC) e remover persistências identificadas em endpoints e servidores. • Validar integridade de backups e selecionar ponto de restauração seguro (RPO) para sistemas essenciais. • Mapear impactos no negócio e priorizar serviços por criticidade (RTO) para a estratégia de retorno.
12–24h	• Restaurar ambientes críticos em modo controlado (staging/blue-green), com hardening mínimo: MFA, least privilege e segmentação. • Aplicar correções definitivas (patch de vulnerabilidade, ajuste de WAF, regras SIEM) antes de reabrir serviços ao público. • Iniciar comunicação externa preliminar (clientes/fornecedores) com transparência: o que ocorreu, o que foi controlado e próximos passos.

24–48h	• Recuperar serviços essenciais (autenticação, ERP/CRM, atendimento) e executar testes de validação funcional e de segurança. • Operar em “modo degradado” se necessário (limites, filas, desligar features sensíveis) para reduzir risco durante a estabilização. • Acionar jurídico/DPO para notificações formais (autoridade e titulares) conforme obrigação legal e orientar suporte ao cliente.
48–72h	• Reintegrar sistemas secundários e integrações, garantindo consistência de dados e monitoramento reforçado (SIEM/alertas). • Revisar e aprovar mensagens definitivas ao público: medidas adotadas, recomendações ao cliente (troca de senha, cuidado com phishing). • Ativar plano de contenção de reputação: central de dúvidas, FAQs, scripts de atendimento e monitoramento de redes/mídia.
3–5 dias	• Realizar revisão completa de acessos (IAM), remover permissões excessivas e implementar políticas de senha/MFA para toda a org. • Executar testes pós-recuperação (pentest focado, varredura contínua) e corrigir achados com prazo e responsável. • Formalizar lições aprendidas, atualizar playbooks e treinar times para reduzir recorrência (table-top + simulado).
5–7 dias (Operação normalizada)	• Declarar normalização quando KPIs/SLA estiverem estáveis e não houver indícios de nova exfiltração por um período definido. • Encerrar a fase de crise com relatório executivo: causa raiz (quando possível), impactos, custos e plano de melhorias. • Manter monitoramento contínuo e auditoria, com roadmap de segurança (DLP, classificação de dados, backups imutáveis, etc.).