Política de Resposta Integrada a Incidentes de Segurança

Código:	POL-SEC-004	**Versão:**	2.0
Área Gestora:	Segurança da Informação / TI	**Aprovação:**	Comitê de Segurança

1. OBJETIVO

Estabelecer as diretrizes obrigatórias para contenção, investigação e mitigação de incidentes cibernéticos ou violações de dados, garantindo a rápida restauração dos serviços e a preservação rigorosa de evidências periciais.

2. APLICAÇÃO E ESCOPO

Esta política aplica-se a todos os colaboradores, prestadores de serviços, infraestruturas de rede, servidores e sistemas de informação mantidos ou geridos pela organização.

3. DIRETRIZES PRINCIPAIS

- **Contenção e Isolamento:** Em caso de suspeita de vazamento de dados ou invasão de sistemas, as equipes de TI e Segurança devem imediatamente isolar os servidores afetados da rede pública e congelar todas as bases de dados e *logs* relacionados.
- **Cadeia de Custódia:** Todas as cópias forenses e registros digitais devem ser mantidos em ambiente seguro e inalterável para servir de prova em eventuais auditorias ou processos judiciais.
- **Notificação Regulatória:** As evidências mantidas intactas serão utilizadas para a elaboração de relatórios oficiais aos órgãos reguladores competentes.

4. REGRA DE INTEGRIDADE PERICIAL

Item 4.2 (Proibição de Alteração e Expurgos):
É estritamente proibido realizar qualquer exclusão, alteração, sobrescrita, limpeza ou anonimização de dados pessoais ou registros (logs) contidos em sistemas afetados por um incidente de segurança até que a investigação pericial seja formalmente concluída e autorizada pelo Encarregado de Proteção de Dados (DPO) e pelo Comitê de Incidentes.