

RELATÓRIO TÉCNICO DE INCIDENTE DE SEGURANÇA - OPERADOR DE DADOS

ORIENTAÇÃO DE GOVERNANÇA E LGPD:

1. Notificação Imediata: o alerta emergencial inicial deve ser feito no ato da detecção pelo Formulário de Comunicação Externa.
2. Relatório Técnico (até 12 horas): este documento deve ser enviado em até 12 horas para o e-mail: dpo@epagri.sc.gov.br com os dados técnicos e evidências.
3. Informações complementares: o DEGTI e o DPO poderão solicitar informações complementares sobre o incidente, que deverão ser informadas imediatamente.

SEÇÃO 1: IDENTIFICAÇÃO DO OPERADOR E CONTRATO

Razão Social do Operador: [Nome empresarial completo]

CNPJ: [00.000.000/0000-00] |

Contrato/Convênio Epagri: [Número do processo SGP-e/Contrato]

Unidade Gestora / Fiscal na Epagri: [Nome do setor/fiscal na Epagri]

Responsável Técnico / DPO do Operador: [Nome, E-mail e Telefone 24h]

SEÇÃO 2: LINHA DO TEMPO E CRONOGRAMA DO INCIDENTE

- **Data/Hora da Ocorrência:** [DD/MM/AAAA às HH:MM]
- **Data/Hora do Conhecimento pelo Operador:** [DD/MM/AAAA às HH:MM]
- **Data/Hora do Alerta Inicial à Epagri:** [DD/MM/AAAA às HH:MM]
- **Data/Hora da Contenção Técnica:** [DD/MM/AAAA às HH:MM ou Em andamento]

Descrição da Dinâmica dos Fatos:

[Detalhamento narrativo de como a falha foi identificada e contida pela equipe técnica do operador]

SEÇÃO 3: CAUSA-RAIZ E DIAGNÓSTICO TÉCNICO FORENSE

- **Classificação do Vetor de Ataque:** [] Ransomware [] Malware [] Falha de Software [] Phishing/Credenciais [] Vazamento de E-mail [] Outro

Outro: [descreva]

- **Vulnerabilidade Técnica Explorada:** [Descrição da falha técnica, porta,

credencial ou código de vulnerabilidade]

• **Ativos e Infraestrutura Comprometida:** [Endereços IP, MAC, nomes de servidores e tabelas atingidas] •

Responsável pela Extração de Logs e Hashes: [Nome do técnico, cargo e hashes de integridade das evidências]

SEÇÃO 4: DIMENSIONAMENTO DOS DADOS PESSOAIS ENVOLVIDOS

• **Confirmação de Envolvimento de Dados Pessoais:** ☐ SIM ☐ NÃO ☐ EM APURAÇÃO

Categorias de Dados Atingidos: ☐ Cadastrais ☐ Documentos ☐ Financeiros ☐ Senhas/Tokens ☐ Dados Sensíveis ☐ Geolocalização

Detalhamento dos dados pessoais atingidos: descreva todos os dados pessoais atingidos [ex: nome, CPF, endereço, filiação, atestados médicos, biometria, etc]

• **Quantidade Estimada de Registros / Linhas:** [ex.: 15.000 linhas de banco de dados]

• **Total de Titulares do Banco de Dados Afetado:**

• **Discriminação de Vulneráveis:** Crianças: [Qtd] | Adolescentes: [Qtd] | Idosos: [Qtd]. Caso não atinja nenhum dos grupos, marque [0]

SEÇÃO 5: CONSEQUÊNCIAS PRÁTICAS E IMPACTOS TÉCNICOS OBSERVADOS

• **Consequências Práticas Observadas:**

☐ Indisponibilidade temporária de sistema/serviço

☐ Exposição de credenciais ou senhas

☐ Alteração não autorizada de registros

☐ Perda definitiva de dados sem backup

☐ Outro. Detalhe [].

☐ Nenhuma consequência operacional identificada

• **Detalhamento dos Impactos Operacionais:** [Descreva os prejuízos operacionais imediatos constatados no ambiente do fornecedor]

SEÇÃO 6: MEDIDAS DE SEGURANÇA E RECUPERABILIDADE

• **Estado de Proteção Anterior:** ☐ Criptografado ☐ Pseudonimizado ☐ Sem proteção especial

Classificação da Recuperabilidade do Sistema: ☐ Regular ☐ Suplementada ☐ Estendida ☐ Não Recuperável. Definições:

- Regular: o tempo de recuperação é previsível com os recursos existentes;
- Suplementado: o tempo de recuperação é previsível, mas exige o empenho de recursos adicionais;
- Estendido: o tempo de recuperação é imprevisível, sendo necessários recursos adicionais e ajuda externa;
- Não Recuperável: a recuperação do incidente não é possível (ex: dados já expostos publicamente).

• **Ações de Contenção e Mitigação Aplicadas:** [Troca de senhas, isolamento de rede, aplicação de patches, etc.]

• **Cronograma de Ações Corretivas Definitivas:** [Listar melhorias de segurança com prazos e responsáveis]

SEÇÃO 7: TERMO DE RESPONSABILIDADE E ASSINATURA

Declaramos que as informações prestadas refletem com exatidão os fatos técnicos apurados, estando cientes de que a avaliação final do risco, a aplicação da Matriz de Impacto da LGPD e a decisão sobre notificações regulatórias cabem exclusivamente ao Encarregado de Dados (DPO) e à Alta Gestão da Epagri.

Representante Legal / Encarregado de Dados Pessoais do Operador
Assinatura Digital (Gov.br / ICP-Brasil)