Do Alerta à Evidência

Metodologia de Investigação DFIR para Eventos Envolvendo Dados Sensíveis

Andrews Moraes

Resposta a Incidentes & Forense Digital

CSIRT | DFIR | LGPD

Disclaimer: Apresentação de caráter técnico e educacional. Os cenários apresentados são fictícios ou devidamente anonimizados.Framework conceitual baseado em DFIR.

- *Casos, métricas e playbooks meramente ilustrativos.*
- *Não representa procedimentos internos de qualquer organização.*
- *Baseado em normas públicas (NIST, ISO, LGPD e ANPD).*

AGENDA

Estrutura da Apresentação |

01 **Sobre o Palestrante**
Contexto profissional e formação

02 **Contexto e Motivação**
Cenário regulatório e desafios atuais

03 **O Problema Central**
Distinguir legítimo de anômalo

04 **Metodologia Proposta**
Framework DFIR para dados sensíveis

05 **Fase 1: Detecção e Triagem**
Do alerta à decisão de investigar

06 **Fase 2: Investigação Forense**
Coleta, análise e correlação

07 **Fase 3: Avaliação de Impacto**
Perspectiva de proteção de dados

08 **Forense Estocástica**
Indícios quando o artefato direto não existe

09 **Falsos Positivos e Priorização**
Tuning, risco e SLAs

10 **~~Caso Prático e Playbooks~~**
Da técnica à decisão

11 **Integração e Métricas**
CSIRT, DPO e KPIs

12 **Fontes e Encerramento**
Referências e perguntas

SEÇÃO 01

Contexto e Motivação

Por que investigações envolvendo dados sensíveis são diferentes?

71%

das organizações sofreram incidentes com dados pessoais, 600 organizações analisadas no relatório IBM Cost of a Data Breach 2025

R$ 7,19M

custo médio de uma violação de dados no Brasil (IBM, 2025)

241 dias

tempo médio global para identificar e conter uma violação

3 dias úteis

Até 3 dias úteis, quando aplicável, conforme regulamentação vigente da ANPD.

A convergência entre volume crescente de dados pessoais, regulamentação rigorosa e sofisticação de ameaças exige abordagens especializadas de investigação.

Fontes: [IBM-2025] [ANPD-CIS] [LGPD]

TLP:CLEAR

SEÇÃO 01

Pressão Regulatória e Compliance

Obrigações legais que impactam a investigação de incidentes

LGPD – Lei Geral de Proteção de Dados

- Art. 46 – Medidas de segurança para proteção de dados
- Art. 48 – Comunicação de incidentes à ANPD e ao titular
- Art. 50 – Boas práticas e governança
- Resolução CD/ANPD nº 15 – Prazos de notificação
- Necessidade de demonstrar diligência investigativa
- Registro e preservação de evidências para accountability

Consequências da Ausência de um Processo Investigativo Estruturado

- Sanções administrativas (multa de até 2% do faturamento)
- Exposição reputacional e perda de confiança
- Impossibilidade de demonstrar conformidade
- Redução da capacidade de sustentar tecnicamente procedimentos administrativos ou judiciais.
- Perda de evidências por má preservação
- Dificuldade na tomada de decisão quanto à comunicação regulatória.

Fontes: [LGPD] [ANPD-CIS]

TLP:CLEAR

SEÇÃO 02

O Problema Central

Quando o acesso legítimo se confunde com o comportamento anômalo.

ACESSO LEGÍTIMO

- Usuário autorizado no sistema
- Função requer acesso a dados
- Padrão consistente de uso
- Volume compatível com a atividade

ZONA CINZENTA

- Volume atípico de consultas
- Horários incomuns de acesso
- Dados fora do escopo funcional
- Padrões não recorrentes

ACESSO INDEVIDO

- Acesso sem necessidade funcional
- Exfiltração comprovada
- Uso de credenciais comprometidas
- Violação de política de acesso

O principal desafio do CSIRT é operar na zona cinzenta: determinar se um comportamento aparentemente legítimo constitui, de fato, uma violação. Isso exige metodologia, evidências e contexto.

SEÇÃO 02

Desafios Específicos do CSIRT

Obstáculos na investigação de eventos com dados sensíveis

Detecção Ambígua

Alertas de DLP e UEBA geram alto volume de falsos positivos em ambientes onde acesso massivo a dados é operacionalmente legítimo

Volume vs. Contexto

Milhões de logs de acesso sem metadados contextuais suficientes para determinar intenção ou necessidade funcional

Necessidade de resposta tempestiva

Prazos regulatórios de notificação (ANPD) exigem conclusões rápidas, enquanto a investigação forense demanda rigor e tempo

Multidisciplinaridade

Necessidade de integração entre equipes de SI, jurídico, compliance, RH e proteção de dados para contextualizar achados

Cadeia de Custódia

Preservação de evidências digitais com integridade para suportar eventual processo administrativo ou judicial

Proporcionalidade

Balancear profundidade investigativa com privacidade dos envolvidos e princípio da minimização

Fontes: [ANPD-CIS] [LGPD]

TLP:CLEAR

SEÇÃO 03

Metodologia Proposta – Visão Geral

Framework integrado: CSIRT + DFIR + Proteção de Dados

FASE 1
DETECÇÃO & TRIAGEM

Alerta → Decisão de Investigar

- Recepção do alerta
- Análise preliminar
- Classificação de risco
- Decisão de escalar

FASE 2
INVESTIGAÇÃO FORENSE (DFIR)

Coleta → Análise → Correlação

- Preservação de evidências
- Análise de logs e artefatos
- Timeline de eventos
- Correlação de fontes

FASE 3
AVALIAÇÃO DE IMPACTO

Evidências → Conclusão → Recomendação

- Classificação dos dados
- Abrangência do acesso
- Avaliação de dano potencial
- Recomendação à gestão

Fontes: [NIST-800-61r3] [NIST-800-122]

TLP:CLEAR

SEÇÃO 04

Fase 1: Detecção e Triagem

Do alerta à decisão de investigar

1

Recepção do Alerta

Fontes: SIEM, DLP, UEBA, denúncias, auditoria interna, comunicação de parceiros

2

Enriquecimento Contextual

Quem é o usuário? Qual sua função? Os dados acessados são compatíveis com suas atribuições?

3

Análise de Risco Preliminar

Classificação: dados pessoais? Sensíveis? Volume? Criticidade? Regulamentações aplicáveis?

4

Decisão de Escalar

Critérios objetivos para abertura de investigação formal vs. encerramento com registro

Ficha de Triagem

Fontes: [LGPD] [NIST-800-122]

TLP:CLEAR

SEÇÃO 05

Fase 2: Investigação Forense – Preservação

Garantindo a integridade das evidências digitais

Fontes de Evidência

- Logs de acesso ao banco de dados
- Logs de aplicação (camada de negócio)
- Registros de autenticação (SSO/MFA)
- Logs de proxy/firewall
- DLP – Data Loss Prevention
- Registros de e-mail e colaboração
- Metadados de arquivos exportados
- Imagens forenses de estações

Cadeia de Custódia Digital

- Hash SHA-256 de cada evidência coletada
- Registro de data/hora da coleta (UTC)
- Identificação do responsável pela coleta
- Armazenamento em repositório protegido
- Ex.: EV-EXEMPLO app_access.log

SHA-256: 9f86d081... (truncado)

Coleta: AAAA-MM-DD

- Conformidade com ISO 27037 e RFC 3227

Ferramentas e Técnicas

- SIEM – Correlação de eventos
- EDR – Análise de endpoints
- Forense de memória (Volatility)
- Análise de logs (Splunk/GC)
- Scripts de automação (Python)
- Análise de metadados de arquivos
- Timeline analysis (Plaso/log2timeline)

Fontes: [ISO-27037] [RFC-3227]

TLP:CLEAR

SEÇÃO 05

Forense Estocástica

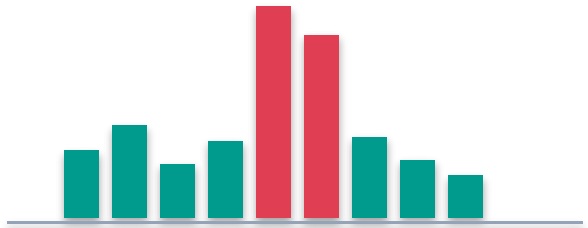
Quando o artefato direto não existe, padrões estatísticos ainda podem falar

Conceito

- Reconstrói atividade digital por propriedades emergentes
- Busca padrões estatísticos em vez de um único artefato
- É útil em suspeitas de insider e cópia silenciosa
- Não substitui DFIR tradicional: complementa a hipótese

Exemplo Técnico

- Cópia massiva pode alterar a distribuição de M.A.C times (***Modificação*** *(mtime),* ***Acesso*** *(atime) e* ***Criação/Mudança*** *(ctime))*
- Um cluster abrupto de acessos pode indicar bulk copy (*Copia em massa*)
- O horário provável vira hipótese investigativa



Cluster de timestamps: indício, não prova isolada

Desafios

- Evidência é probabilística e precisa de corroboração
- Baseline ruim aumenta falso positivo
- Timestamps podem ser desabilitados, normalizados ou alterados
- Atividades legítimas também podem gerar padrões parecidos
- Requer analista treinado e documentação da hipótese

Uso recomendado: levantar hipótese, orientar coleta adicional e confirmar com logs, DLP, endpoint, autenticação e contexto de negócio.

Fontes: [GRIER-2011] [NIST-800-61r3]

TLP:CLEAR

SEÇÃO 06

Fase 3: Avaliação de Impacto

Perspectiva de proteção de dados pessoais

MATRIZ DE AVALIAÇÃO DE IMPACTO

CRITÉRIO	ANÁLISE	PESO
Natureza dos Dados	Dados pessoais sensíveis (saúde, biometria) ou dados comuns	ALTO
Volume Afetado	Número de titulares cujos dados foram efetivamente acessados	MÉDIO-ALTO
Possibilidade de Identificação	Dados permitem identificar diretamente o titular?	ALTO
Consequências ao Titular	Risco de dano patrimonial, moral, discriminação	CRÍTICO
Reversibilidade	É possível mitigar os efeitos do acesso indevido?	MÉDIO
Circunstâncias do incidente	O controlador adotou medidas razoáveis de proteção?	ATENUANTE

Referências

- LGPD Art. 44, 46 e 48
- ANPD – Formulário de CIS
- NIST SP 800-122
- NIST SP 800-61 Rev. 3
- ISO 27701:2019

Fontes: [LGPD] [ANPD-CIS] [NIST-800-122] [ISO-27701]

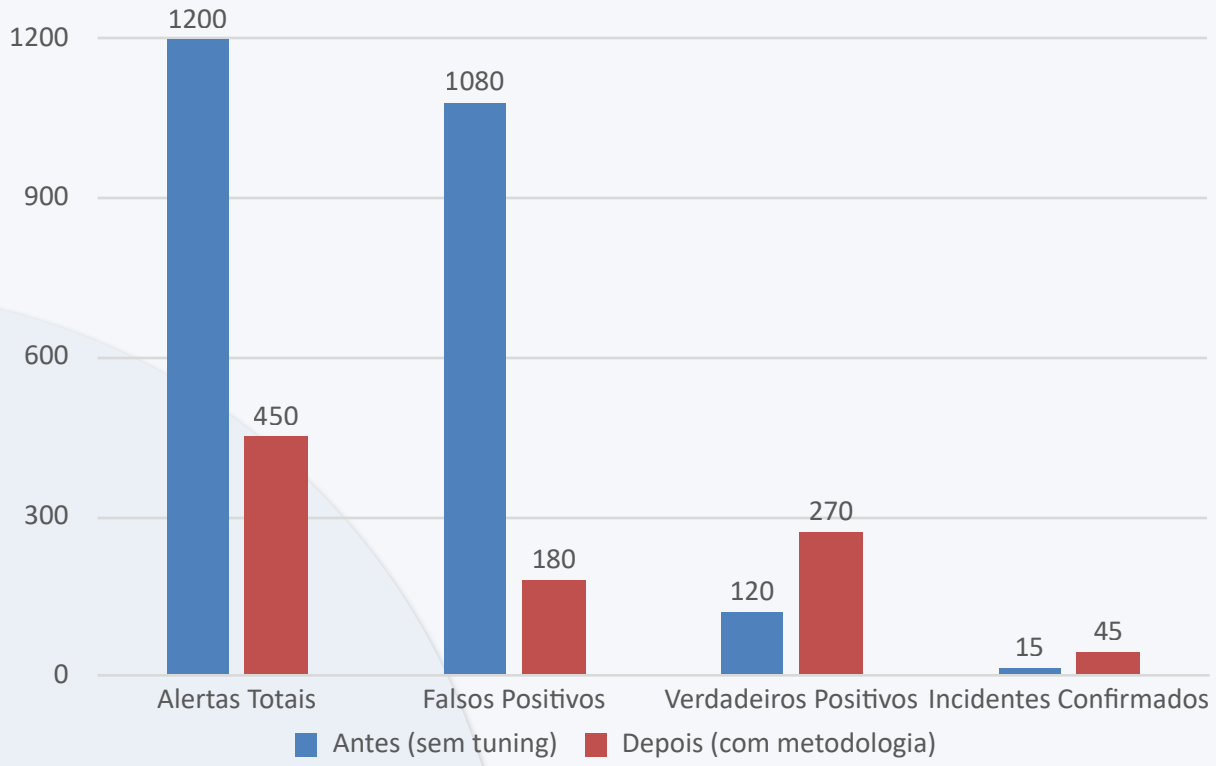
TLP:CLEAR

SEÇÃO 07

Da Fadiga de Alertas à Investigação Qualificada

Estratégias para melhorar a precisão da detecção

Simulação didática para demonstrar efeito de tuning e enriquecimento contextual.



Dados meramente ilustrativos.

Baseline Comportamental

Estabelecer padrões de acesso normal por função/cargo antes de definir thresholds de alerta

Contextualização Automática

Enriquecer alertas com dados de diversas fontes (RH - cargo, departamento, período de emprego) para pré-filtrar

Whitelisting Inteligente

Regras dinâmicas para atividades legítimas recorrentes, com revisão periódica

Scoring Multifatorial

Pontuar alertas com múltiplos indicadores ao invés de regras binárias simples

Rastreabilidade e cadeia de custódia

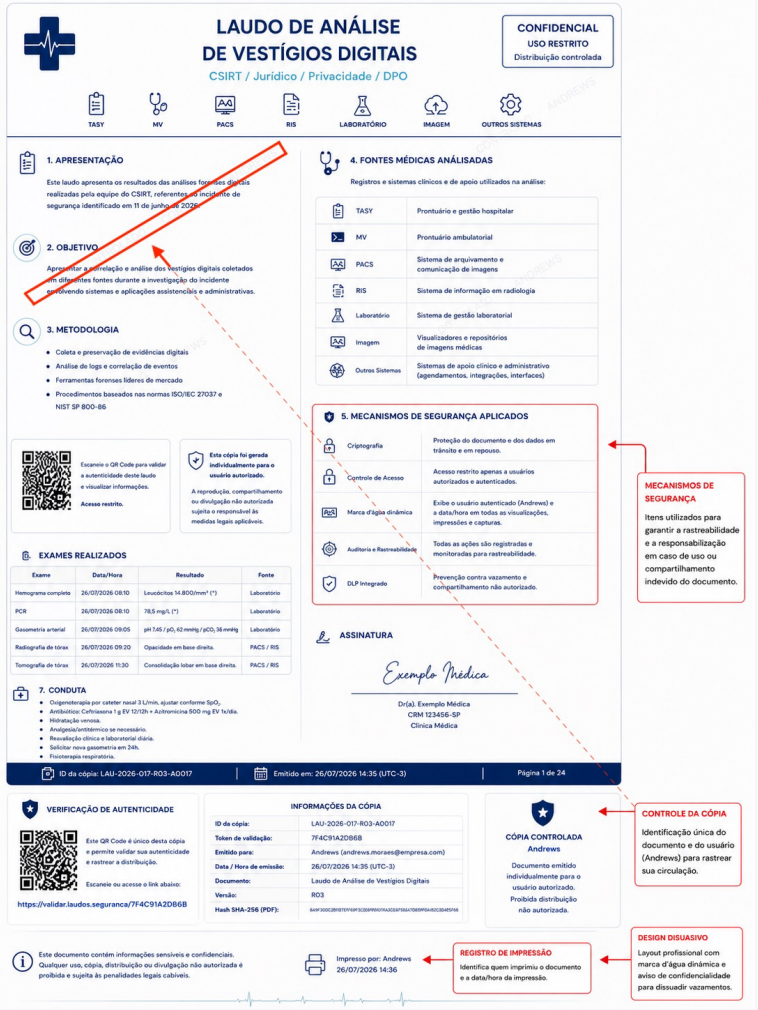
Conjunto de procedimentos formais para documentar a história cronológica de um vestígio.

Base: [NIST-800-61r3]

TLP:CLEAR

SEÇÃO 07

Redução de Falsos Positivos e Rastreabilidade



Modelo de exemplo

Dados meramente ilustrativos.

Base: [NIST-800-61r3]

TLP:CLEAR

SEÇÃO 07

Priorização de Incidentes

Framework de classificação baseado em risco e impacto

MATRIZ DE PRIORIZAÇÃO

SENSIBILIDADE DOS DADOS ↑	ANOMALIA COMPORTAMENTAL →		
Dados Sensíveis	**P3** MÉDIA	**P2** ALTA	**P1** CRÍTICA
Dados Pessoais	**P4** BAIXA	**P3** MÉDIA	**P2** ALTA
Dados Comuns	**P4** BAIXA	**P4** BAIXA	**P3** MÉDIA

SLA por Prioridade (metas sugeridas)

P1 – CRÍTICA: Resposta imediata (<30m), investigação em 24h

P2 – ALTA: Triagem em 1h, investigação em 48h

P3 – MÉDIA: Triagem em 2h, investigação em 3 dias úteis

P4 – BAIXA: Registro e análise em batch semanal

Fatores de aceleração:

→ Dados de menores de idade

→ Dados de saúde / biométricos

→ Evidência de exfiltração confirmada

→ Suspeita de insider threat ativo

Dados meramente ilustrativos.

Base: [LGPD] [ANPD-CIS] [NIST-800-61r3]

TLP:CLEAR

SEÇÃO 08

Playbooks Específicos

Procedimentos estruturados para investigações com dados sensíveis

PB-001 Acesso Massivo a Dados Pessoais

1. Trigger: Consulta > 5x baseline
2. Verificar justificativa funcional
3. Analisar exportações associadas
4. Validar com gestor imediato
5. Documentar e classificar

PB-002 Exfiltração Suspeita de Dados

1. Trigger: DLP/proxy alert
2. Avaliar contenção imediata conforme criticidade.
3. Preservar evidências
4. Análise forense do endpoint
5. Notificar DPO e jurídico

PB-003 Insider Threat com Dados Sensíveis

1. Trigger: Correlação UEBA+RH
2. Investigação sigilosa inicial
3. Monitoramento reforçado conforme política institucional e legislação aplicável.
4. Análise de acessos retroativos
5. Relatório para comitê de crise

PB-004 Acesso Indevido por Privilégios Excessivos

1. Trigger: Auditoria de acessos
2. Mapear acessos vs. função
3. Identificar dados expostos
4. Revisar privilégios e aplicar o princípio do menor privilégio.
5. Avaliar impacto retroativo

Base: [NIST-800-61r3] [ISO-27035]

TLP:CLEAR

SEÇÃO 10

Integração CSIRT + Proteção de Dados

Modelo de referência para investigações conjuntas

CSIRT

- Monitoramento contínuo (24x7)
- Detecção e triagem de alertas
- Investigação forense digital
- Preservação de evidências
- Análise técnica de artefatos
- Contenção e erradicação
- Timeline e relatório técnico

COMUNICAÇÃO ESTRUTURADA

→ Critérios de escalação definidos

→ Templates de relatório padronizados

→ SLA de comunicação acordado

→ Reuniões de alinhamento periódicas

DPO / PRIVACIDADE

- Classificação dos dados envolvidos
- Avaliação de impacto ao titular
- Análise de obrigação de notificação
- Comunicação com ANPD
- Comunicação com titulares
- Registro no ROPA
- Lições aprendidas de privacy

Base: [NIST-800-61r3] [ANPD-CIS]

TLP:CLEAR

SEÇÃO 10

Indicadores e Métricas

KPIs para medir a efetividade do processo investigativo

Exemplos de metas de referência para maturidade inicial; ajustar conforme porte, risco e obrigação regulatória.

MTTD — Mean Time to Detect

Tempo médio entre o evento e o primeiro alerta

< 5MIN

MTTR — Mean Time to Respond

Tempo total do alerta à contenção

< 30M

MTTI — Mean Time to Investigate

Tempo médio para conclusão da investigação forense

< 48H

FPR — False Positive Rate

Percentual de alertas que não se confirmam

< 30%

ECR — Evidence Completeness

% de investigações com cadeia de custódia completa

> 95%

NTR — Notification Timeliness

% de notificações à ANPD dentro do prazo regulatório

100%

Metas de referência para organizações com processo maduro. Devem ser adaptadas conforme o contexto operacional.

Base: [NIST-800-61r3] [ANPD-CIS]

TLP:CLEAR

SEÇÃO 10

Lições Aprendidas

Evolução do processo de resposta a incidentes

01 Contexto é Primordial

A análise puramente técnica de logs é insuficiente. Informações de RH, gestão e negócio são essenciais para determinar se um acesso é legítimo ou anômalo.

02 Playbooks Salvam Tempo

Procedimentos pré-definidos e testados reduzem o MTTI e garantem consistência independentemente do analista.

03 Falso Positivo Custa Caro

Cada falso positivo consome tempo de analista, gera fadiga operacional e reduz foco em eventos de maior risco.

04 Preservação desde o Início

Evidências mal preservadas nos primeiros minutos podem inviabilizar toda a investigação e qualquer ação legal posterior.

05 Integração Contínua

A parceria entre CSIRT e DPO não deve ocorrer apenas durante incidentes. Treinamentos conjuntos e simulações regulares são fundamentais.

06 Documentação é Defesa

Em caso de questionamento pela ANPD, a qualidade da documentação do processo investigativo é tão importante quanto o resultado.

Base: [NIST-800-61r3] [ANPD-CIS]

TLP:CLEAR

SEÇÃO 10

Recomendações

Ações práticas para organizações

CURTO PRAZO (0–4 meses)

- Mapear fontes de dados sensíveis no ambiente (Data Mapping - ROPA)
- Definir baselines de acesso por função/ cargo - SoD
- Criar playbook
- Estabelecer canal CSIRT ↔ DPO
- Revisar regras de DLP

MÉDIO PRAZO (4–12 meses)

- Implementar scoring multifatorial de alertas
- Automatizar enriquecimento contextual (RH/IAM)
- Treinar equipe com foco em privacidade
- Simular cenários de incidente com dados sensíveis - Tabletop
- Estabelecer métricas e dashboard de KPIs

LONGO PRAZO (12+ meses)

- Programa de maturidade contínua (CMMI)
- Avaliar adoção de IA/ML
- Expandir playbooks para todos os cenários
- RBAC + SoD
- Benchmarking com organizações do setor

Base: [NIST-800-61r3] [ISO-27035] [ISO-27701]

TLP:CLEAR

Conclusão

Não existe metodologia única; o framework deve ser adaptado ao contexto de cada organização.

A combinação metodológica de CSIRT, DFIR e avaliação de impacto sob a ótica de proteção de dados permite às organizações:

- ✦ Responder com mais rapidez e precisão a eventos envolvendo dados pessoais
- ✦ Reduzir falsos positivos e otimizar recursos de investigação
- ✦ Atender requisitos regulatórios com evidências robustas e documentadas
- ✦ Fortalecer a postura de segurança e proteção de dados da organização

A evolução da maturidade nesse processo não é um destino, é uma jornada contínua de aprendizado, adaptação e integração entre equipes capacitadas.

Base: [NIST-800-61r3] [ANPD-CIS]

TLP:CLEAR

Obrigado!

Andrews Moraes

Resposta a Incidentes & Forense Digital

As opiniões, metodologias e exemplos apresentados refletem exclusivamente a visão técnica do autor, possuindo finalidade educacional e não representando necessariamente processos, tecnologias ou posicionamentos da instituição à qual esteja vinculado.

Minhas Perguntas a Vocês

- Compartilhe suas experiências com investigações de dados sensíveis
- Como sua organização integra CSIRT e proteção de dados?
- Quais são seus maiores desafios na redução de falsos positivos?

Referências e Leitura Complementar

- NIST SP 800-61 Rev. 3 – Incident Response
- NIST SP 800-122 – PII Confidentiality Guide
- Grier – Stochastic Forensics
- ISO 27035 – Incident Management
- ISO 27037 – Digital Evidence Handling
- Fontes completas no próximo slide

Fontes e Links

Referências usadas para estatísticas, normas, metodologia de resposta e forense estocástica.

[TLP-FIRST] FIRST Traffic Light Protocol

www.first.org/tlp/

[IBM-2025] IBM Cost of a Data Breach Report 2025

brasil.newsroom.ibm.com/2025-07-30-Relatorio-da-IBM-Custo-medio-de-um...

[ANPD-CIS] ANPD - Comunicacao de Incidente de Seguranca

www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunic...

[LGPD] Lei Geral de Protecao de Dados Pessoais

www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[NIST-800-61r3] NIST SP 800-61 Rev. 3

csrc.nist.gov/pubs/sp/800/61/r3/final

[NIST-800-122] NIST SP 800-122

csrc.nist.gov/pubs/sp/800/122/final

[GRIER-2011] Detecting Data Theft Using Stochastic Forensics

dfrws.org/sites/default/files/session-files/2011_USA_paper-detecting_...

[RFC-3227] RFC 3227

datatracker.ietf.org/doc/html/rfc3227

[ISO-27037] ISO/IEC 27037:2012

www.iso.org/standard/44381.html

[ISO-27035] ISO/IEC 27035-1:2023

www.iso.org/standard/78973.html

[ISO-27701] ISO/IEC 27701:2019

www.iso.org/standard/71670.html

Clique nos marcadores para abrir os links completos. Caso prático, query e gráfico de tuning são exemplos didáticos/anonimizados.