Opice Blum

Redefinindo os limites do possível.

cert.br nic.br cgi.br

LIVE

INTRAREDE

2025 — 5 ANOS

ATAQUE DE RANSOMWARE

https://intrarede.nic.br | 06 de Agosto de 2025 - 10h (UTC -3)

Realização

ceptro.br nic.br cgi.br

Guilherme Ochsendorf de Freitas

Especialista em Direito e Tecnologia da Informação pela POLI-USP, MBA em Gestão Estratégica em Tecnologia da Informação pela FEA-RP - USP.

Certificado em Cibersegurança pelo ISC2 e Resposta a Incidente pela Carnegie Mellon University (CERT.br) e FGV.

Advogado do Time de Resposta a Incidentes no Opice Blum e Professor em Cursos de Pós-Graduação em Direito Digital.

https://br.linkedin.com/in/guilhermeochsendorf

TLP:CLEAR

Se vc está vendo esse texto, vc não vai mais conseguir acessar seus arquivos.

Nós somos o grupo hacker SOD1NOK1B1 e criptografamos/roubamos seus arquivos.

É possível que vc esteja em busca de alguma maneira de recuperar seus arquivos.
É desperdício de tempo. Ninguém vai conseguir recuperá-los sem a nossa ajuda.

Nós garantimos para vc que é possível recuperar todos os seus arquivos em segurança. Tudo o que vc tem que fazer é pagar o resgate e receber a chave de descriptografia.

Vc precisa pagar 30 bitcoin no prazo de 24 horas, caso contrário vamos postar seus arquivos na deep web, no endereço caforssztxqzf2nm.onion. Entre em contato no e-mail m0nk3ydluffy@protonmail.com

Se você já obteve sua senha, por favor digite abaixo.
Senha#1: _

Conceitos introdutórios – Comunicação à ANPD

O que é um incidente de segurança e dados pessoais para ANPD?

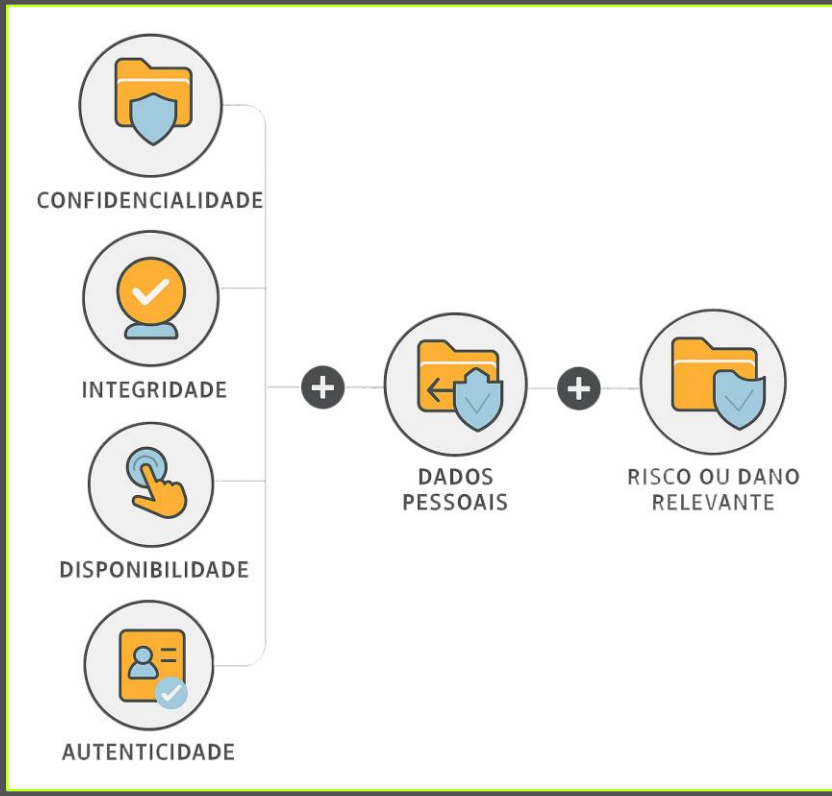
Qualquer evento adverso confirmado que comprometa as propriedades de *confidencialidade, integridade, disponibilidade* ou *autenticidade dos dados pessoais.*

O que é risco ou dano relevante?

Um incidente pode acarretar risco ou dano relevante quando *"puder afetar significativamente interesses e direitos fundamentais dos titulares".*

O que considerar para avaliação do risco do incidente?

- O contexto da atividade de tratamento de dados;
- As categorias e quantidades de titulares afetados;
- As naturezas, as categorias e a quantidade de dados violados;
- Os potenciais danos materiais, morais, reputacionais causados aos titulares; risco de fraude ou engenharia social;
- *As medidas de mitigação adotadas pelo controlador após o incidente.*



TLP:CLEAR

Incidentes de *Ransomware* na ANPD

ANPD

COORDENAÇÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA - TIS
COORDENAÇÃO-GERAL DE FISCALIZAÇÃO - CGF

NÚMERO DE INCIDENTES DE SEGURANÇA RECEBIDOS
2021 - 2025

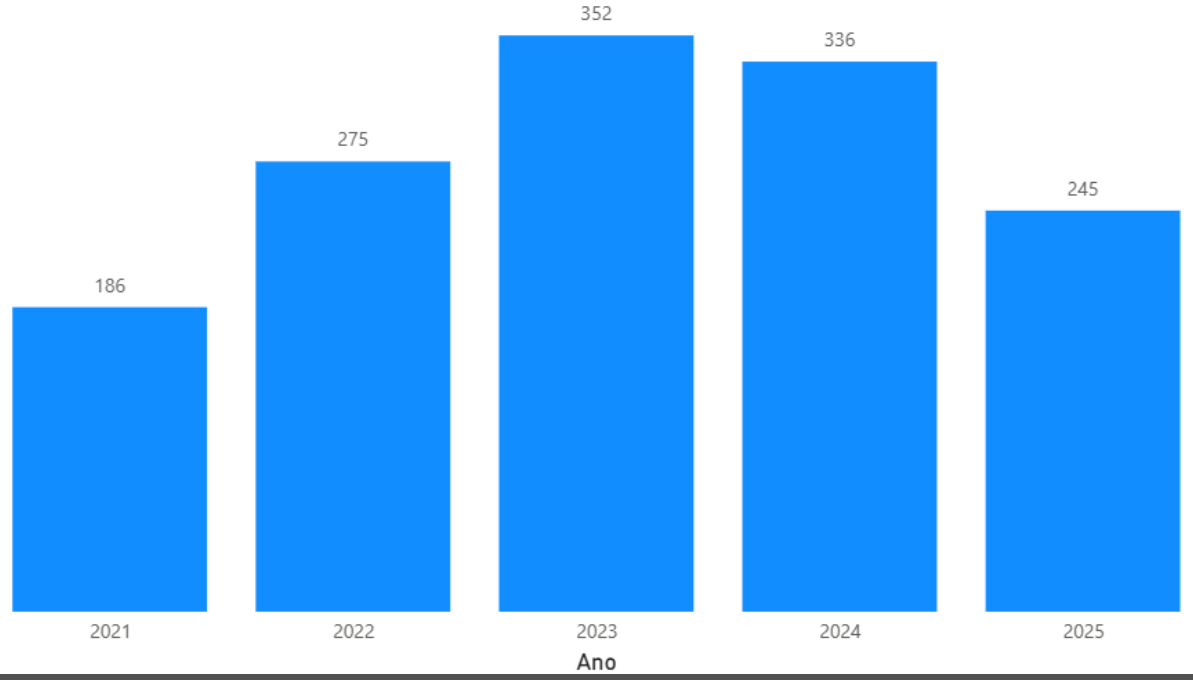
Última Atualização
Atualizado em 06/08/2025 às N/D

Ano, Trimestre, Mês
Todos

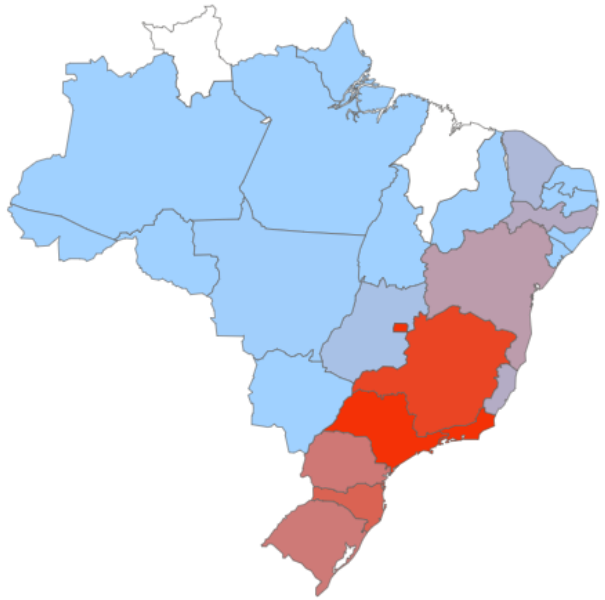
UF
Todos

Incidentes Reportados
1,394 Mil

Incidentes x Ano

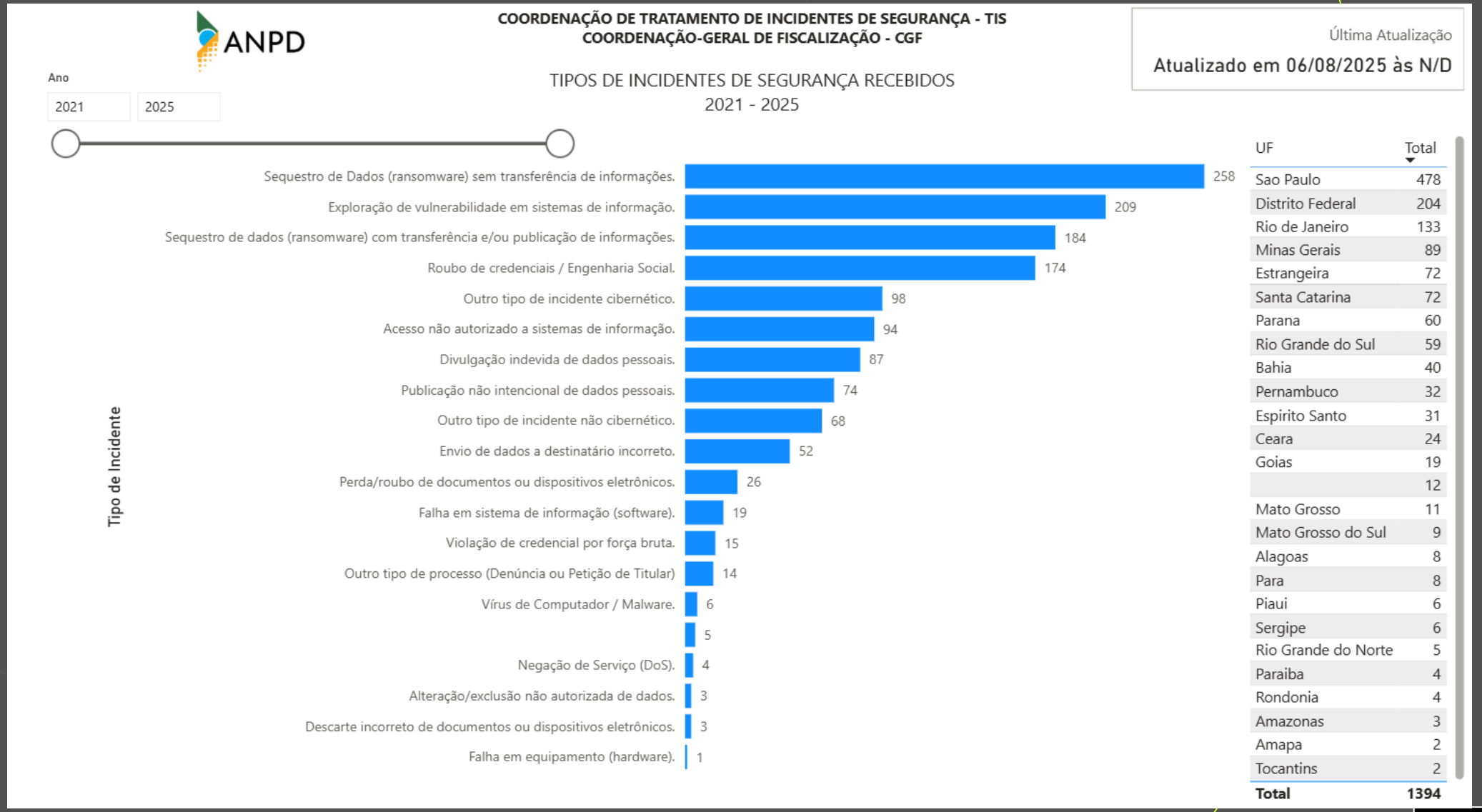


Incidentes por UF
2021 - 2025



TLP:CLEAR

Incidentes de *Ransomware* na ANPD



TLP:CLEAR

Incidentes de *Ransomware* na ANPD

Incidentes de *Ransomware* na ANPD

A importância dos Logs na resposta a incidentes

Por que os logs são essenciais?

- Permitem identificar a causa e a extensão do incidente.
- Ajudam a delimitar o impacto real: o que ocorreu, o que foi acessado ou exfiltrado, quais dados foram violados.
- São fundamentais para a avaliação do risco e definição da obrigação de notificação à ANPD e aos titulares.

Ausência de logs

Pior cenário

- Impõe ao controlador a necessidade de comprovar a origem ou a falsidade das amostras de dados publicadas.
- Exige a delimitação do impacto real: quais sistemas foram comprometidos, quais informações foram expostas e se os dados publicados são autênticos.
- São determinantes para a avaliação da cooperação com a autoridade e para a definição das consequências regulatórias.

TLP:CLEAR

Incidentes de *Ransomware*

Casos de dados não estruturados

Qual abordagem adotar?

- Criação da matriz de risco e para a tomada de decisão sobre a comunicação, seja a todos os titulares, a grupos de risco identificados, ou a documentação da não comunicação.
- Permite identificar os tipos de dados presentes e a extensão do comprometimento dentro do universo de arquivos não estruturados e ajuda a delimitar o impacto.

Medidas técnicas como argumentos de defesa

Medidas de segurança aos dados

O dever de comunicação aos titulares só existe quando o incidente for capaz de "acarretar risco ou dano relevante".

Adotar medidas técnicas eficazes podem eliminar ou reduzir drasticamente esse risco, afastando o dever de comunicação.

- Criptografia
- Anonimzação
- Monitoramento
- Remoção do conteúdo

TLP:CLEAR

Incidentes de *Ransomware*

Realizar o pagamento do resgate:

Prós

- ✓ Possível interrupção do vazamento e minimização de danos aos titulares.
- ✓ Possível obtenção de tempo adicional para respostas técnicas e jurídicas.

Contras

- x Ausência de garantias sobre a não divulgação dos dados.
- x Pagamento pode ser interpretado como incentivo à atividade criminosa e carece de respaldo legal.

Não realizar o pagamento:

Prós

- ✓ Obter informações mais precisas antes da adoção de medidas adicionais.
- ✓ Evita envolvimento direto em prática potencialmente ilegal.

Contras

- x Risco de exposição de informações e de publicidade ao evento.
- x Possível repercussão negativa e perda de confiança pública, inclusive institucional.

Olhar do regulador

Construindo a história de um incidente.

- Identificar o que aconteceu (causa raiz);
- Corrigir as falhas/vulnerabilidades;
- Implementar soluções/correções (contenção, erradicação e recuperação);
- Implementar medidas de mitigação de danos.
- Avaliação de risco do incidente para sustentar ou não a comunicação à ANPD e aos titulares de dados;

Recomendações.

- Logs são ativos críticos que definem o incidente.
- Documentação detalhada subsidiarão a análise jurídica e a tomada de decisão da companhia.
- Integre o jurídico com o time técnico
- Utilize frameworks de referência, tanto de resposta a incidentes como de segurança da informação (NIST, ISO).

TLP:CLEAR

cert.br nic.br cgi.br

Opice BLUM

Guilherme Ochsendorf de Freitas

guilherme.freitas@opiceblum.com.br