Guia de resposta a incidentes de segurança a proteção de dados pessoais

Secretaria de Governo Digital

Setembro/2021

Lei Geral de Proteção de Dados – Lei 13.709/18

Estratégia de Governo Digital 2020-2022 / Um Governo Confiável

Objetivo 10: Implementação da Lei Geral de Proteção de Dados - LGPD no Governo

Iniciativa 10.1: Estabelecer método de adequação e conformidade dos órgãos com os requisitos da Lei Geral de Proteção de Dados, até 2020

Objetivo 11: Garantia da segurança das plataformas de governo digital e de missão crítica

Iniciativa 11.3. Definir padrão mínimo de segurança cibernética a ser aplicado nos canais e serviços digitais.

PROJETO ADEQUAÇÃO À LGPD

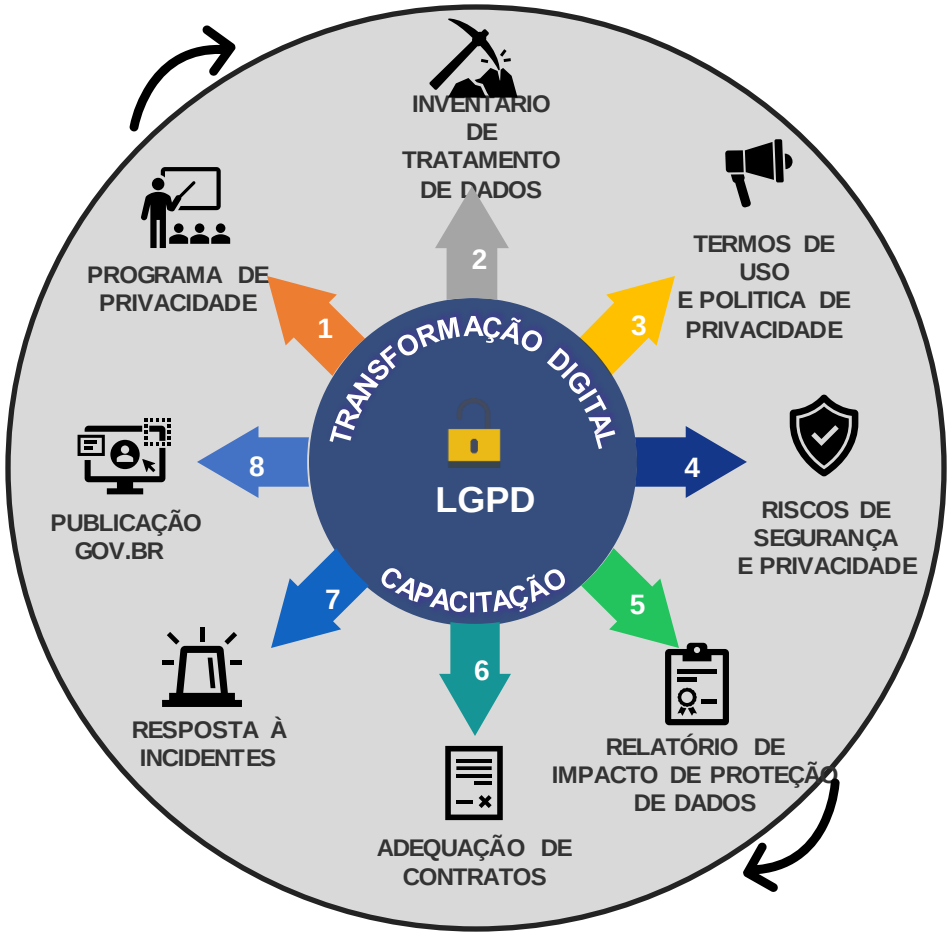
Objetivo: Definir e implementar estratégia para atuar preventivamente nas frentes de segurança da informação e privacidade de dados, com o intuito de fomentar a cultura de proteção de dados, implementando ações que visam avançar no processo de adequação à LGPD, minimizando os riscos.

Objetivo do Guia

- **Fomentar a adequação à Lei Geral de Proteção de Dados Pessoais dentro da administração pública federal;**

- **Auxiliar tanto os profissionais que estão ou que serão designados ao tratamento de dados pessoais nas diversas pastas da administração pública federal (APF), quanto os profissionais responsáveis pelo tratamento de incidentes cibernéticos dessas instituições.**

Oficinas


INVENTÁRIO DE TRATAMENTO DE DADOS
TERMOS DE USO E POLITICA DE PRIVACIDADE
RISCOS DE SEGURANÇA E PRIVACIDADE
RELATÓRIO DE IMPACTO DE PROTEÇÃO DE DADOS
ADEQUAÇÃO DE CONTRATOS
RESPOSTA À INCIDENTES
PUBLICAÇÃO GOV.BR
PROGRAMA DE PRIVACIDADE
1
2
3
4
5
6
7
8
TRANSFORMAÇÃO DIGITAL
LGPD
CAPACITAÇÃO

Agenda

1. Alinhamento de expectativas;
2. Contexto;
3. Referências;
4. Incidente de Segurança com dados pessoais;
5. Resposta a incidentes cibernéticos;

Alinhamento de expectativas

Benefícios

Amadurecimento de processos internos de segurança

Estabelecer processo de resposta a incidentes

Nortear investimentos em segurança

Auxiliar a priorização de demandas

Estabelecer o plano de comunicação

Conformidade legal com a LGPD

Contexto

- **Recorrência de incidentes de segurança;**
- **Instrução normativa nº01 GSI/PR;**
- **Rede Federal de Gestão de Incidentes Cibernéticos (Decreto nº 10.748, de 16 de julho de 2021);**
- **Lei Geral de Proteção de Dados Pessoais, art 48 e 50.**

Contexto

3.000 (72%)
serviços digitais

279 Sistemas de missão crítica na APF

GOV.BR
84 Mi de usuários
70 Mi Visitas/mês

Até 60% de servidores em trabalho remoto

Demanda por digitalização

Riscos de Segurança da Informação e proteção a privacidade

"Novo vazamento de dados do Ministério da Saúde expõe 200 milhões de brasileiros" (12/2020)

"Ataque hacker ao STJ é o pior da história do Brasil" (11/2020)

"Ataque hacker: portal do TRF-1 é tirado do ar como medida preventiva" (12/2020)

$1.12 Mi
Prejuízo médio no Brasil para um vazamento de dados em 2020*

Contexto

Exclusivo: falha em site do Ministério do Trabalho vazou dados de brasileiros

Sistema do antigo Ministério do Trabalho revelava dados pessoais com consulta de CPF; site saiu do ar após notificação do Tecnoblog

Ministério da Saúde identifica "vírus" na rede do DataSUS

Investiga a origem do problema

Não há indícios de ataque hacker

Site do departamento foi bloqueado

Contexto

Vazamento no Ministério da Saúde expõe dados de 16 milhões de pessoas

Base de pacientes de covid-19

Lista tem Bolsonaro e autoridades

Hospital Regional da Asa Norte, referência para a covid-19 em Brasília, pacientes de unidades públicas e privadas foram expostos

PODERIOS
26 nov 2020 (quinta-feira) - 09:10

Hacker invade rede do Ministério da Saúde e avisa que "site está um lixo"

Mensagem do invasor foi apresentada no serviço de criação de formulários do DataSUS. Ministério da Saúde informa que situação foi controlada

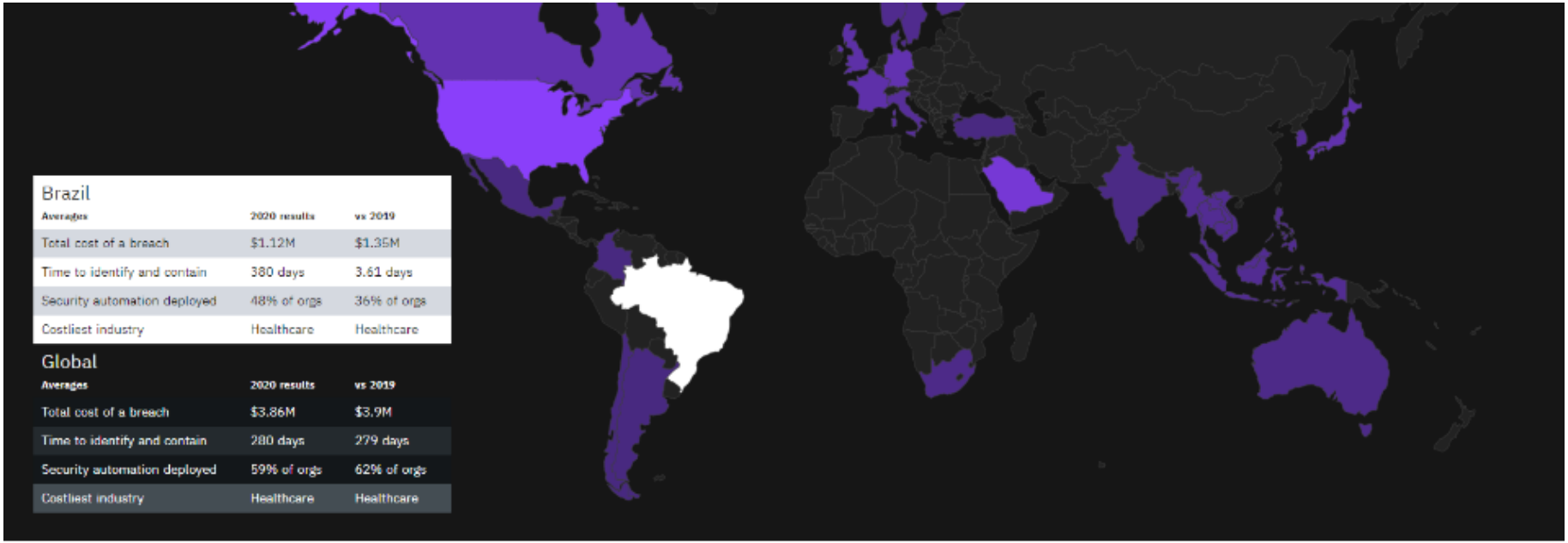
Por Ana Marques

O **Ministério da Saúde** teve sua rede invadida por um hacker na última quinta-feira (28). O ataque, no entanto, não teve como objetivo vazar dados ou causar danos à plataforma – o invasor fez apenas um alerta em relação à vulnerabilidade: "Este site está um lixo!". O caso aconteceu algumas semanas após a descoberta de uma falha de segurança no e-SUS que expôs os dados de mais de 200 milhões de brasileiros na internet.

Contexto

Fonte: https://threatmap.checkpoint.com/

Contexto



Brazil

Averages	2020 results	vs 2019
Total cost of a breach	$1.12M	$1.35M
Time to identify and contain	380 days	3.61 days
Security automation deployed	48% of orgs	36% of orgs
Costliest industry	Healthcare	Healthcare

Global

Averages	2020 results	vs 2019
Total cost of a breach	$3.86M	$3.9M
Time to identify and contain	280 days	279 days
Security automation deployed	59% of orgs	62% of orgs
Costliest industry	Healthcare	Healthcare

Fonte: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pt

Contexto

Brasil 1º em Phishing em 2021

O Brasil teve um aumento de 23% nos casos de cibercrimes nos primeiros oito meses de 2021 em comparação ao mesmo período no ano anterior. Foram 481 milhões de tentativas de infecção com os 20 malwares mais populares.

Kaspersky Lab

Brasil 2º em Phishing em 2021

O Brasil sofreu entre 1º de janeiro e 3 de agosto de 2021 mais de 439.000 ataques cibernéticos, 7,1% de um total de 6,4 milhões realizados em todo o mundo. Os ataques registrados foram do tipo de negação de serviço distribuído (DDoS, na sigla em inglês)

NETSCOUT SYSTEMS, INC.

Brasil 5º em Ransomware em 2021

Só nos seis primeiros meses deste ano, os registros no país já superaram o total de ocorrências de 2020. Se considerados apenas os casos de ransomware, já foram 9,1 milhões de casos em 2021.

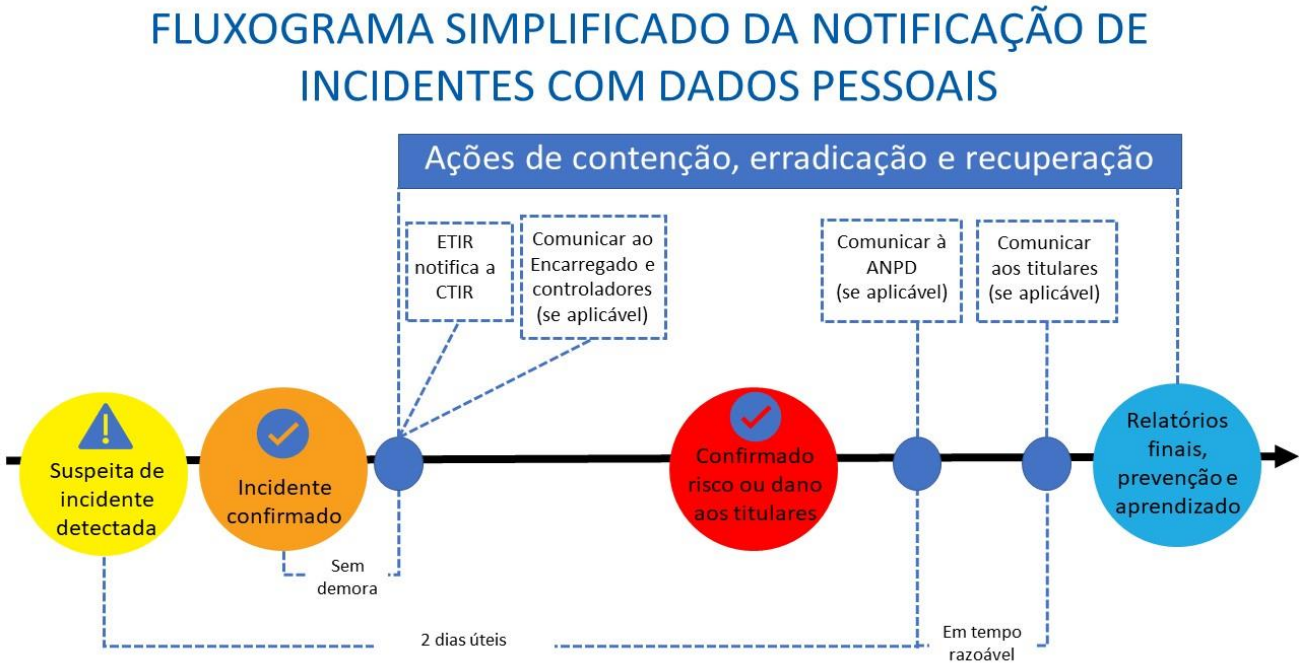
SonicWall Cyber Threat Report

O setor mais atingido por ataques foi o governo, com alta de 917% em relação ao 1° semestre do ano passado.

SonicWall Cyber Threat Report

Principais referências

Incidente com dados pessoais



Incidente com dados pessoais

Incidente com dados pessoais

Comunicação:

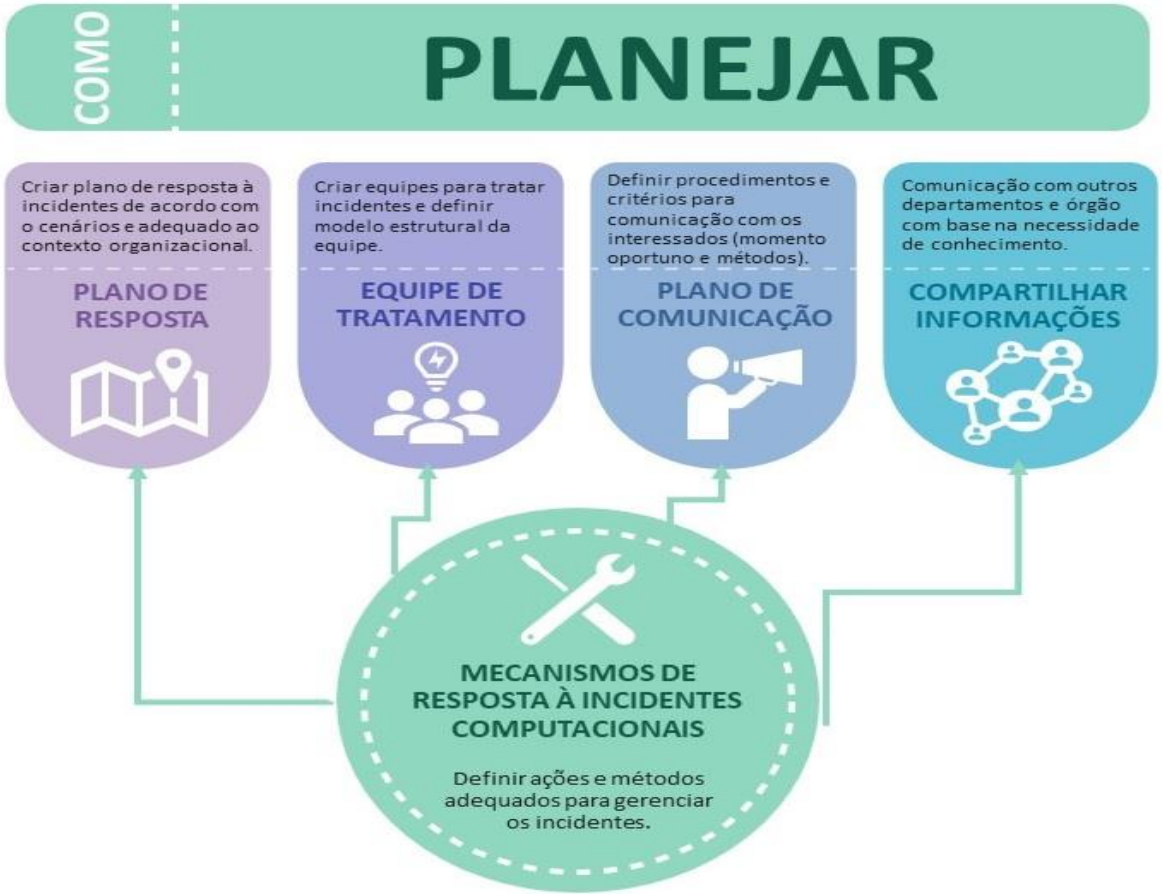
- Encarregado;
- Controlador;
- ANPD;
- Notificar os titulares de dados pessoais;
- ETIR e CTIR Gov;
- Canais de comunicação.

Resposta a incidentes cibernéticos

Rede Federal de Gestão de Incidentes Cibernéticos

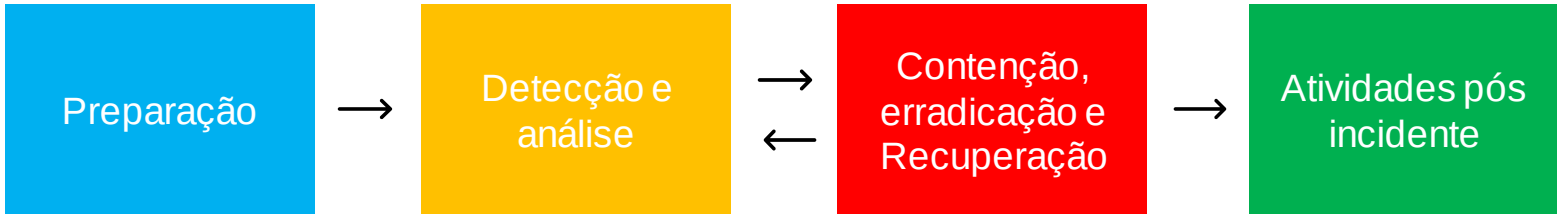
- CTIR Gov;
- Entes da APF;
- Empresas Privadas.

Resposta a incidentes cibernéticos



Resposta a incidentes cibernéticos

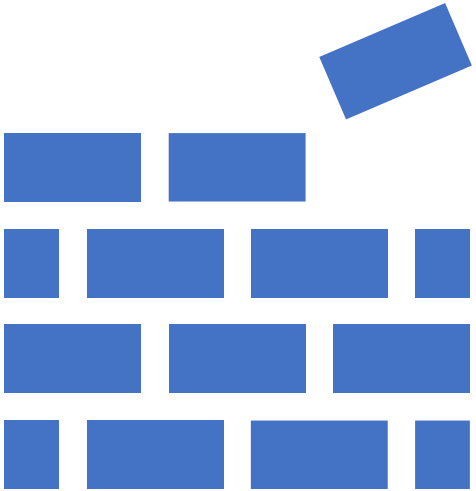
Tratamento de incidentes computacionais



Resposta a incidentes cibernéticos

Preparação

- Ferramentas;
- Prevenção;
- Treinamento;
- Simulações;
- Equipe.



Resposta a incidentes cibernéticos

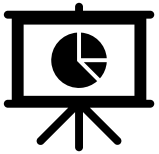
Detecção e análise

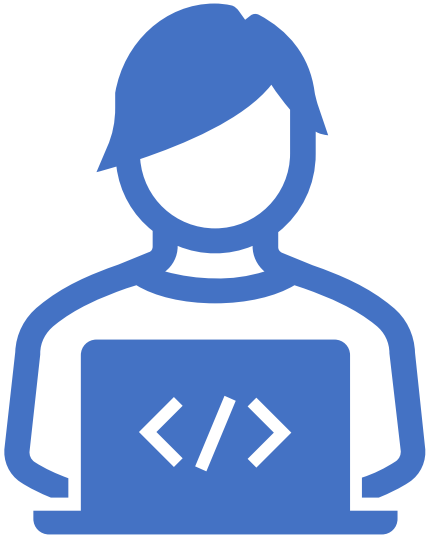
- Monitoração;
- Vetores de ataque;
- Sinais de incidentes;
- Análise;
- Documentação;
- Priorização;
- Notificação.

Resposta a incidentes cibernéticos

Contenção, erradicação e recuperação

- Estratégia de contenção;
- Coleta e manuseio de informações;
- Origem de ataques;
- Análise.

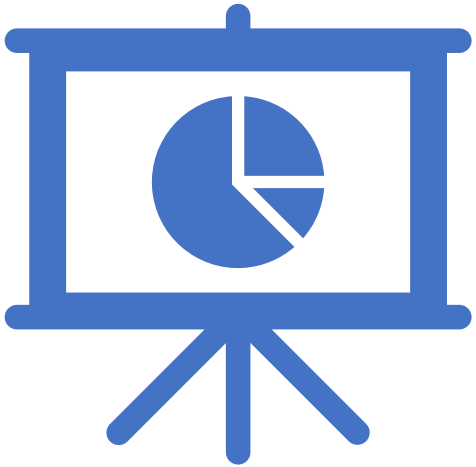




Resposta a incidentes cibernéticos

Atividades pós incidente

- Lições aprendidas;
- Usando dados coletados;
- Retenção de evidência;
- Compartilhamento de informações;
- Recomendações.



Contato

cgsin@economia.gov.br

MINISTÉRIO DA
ECONOMIA

PÁTRIA AMADA BRASIL
GOVERNO FEDERAL

Secretaria de
Governo Digital