SEGURANÇA DOS DADOS E LGPD NA PRÁTICA

PROTEÇÃO DE DADOS NO AMBIENTE DE TRABALHO: CLASSIFICAÇÃO, COMPARTILHAMENTO SEGURO E USO DA NUVEM

MINISTÉRIO DA EDUCAÇÃO
GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

ROTEIRO DA PALESTRA

01

Fundamentos

Pilares da segurança da informação e o que a LGPD exige

02

Classificação da informação

Pública, pessoal, sensível ou sigilosa: como identificar

03

Compartilhamento seguro

Perguntas-chave, canais e os Acordos de Compartilhamento da CAPES

04

Nuvem e armazenamento

Responsabilidade compartilhada, links, contas e IA generativa

05

Casos reais

Causas, impactos e lições aprendidas de exposições de dados

01

FUNDAMENTOS

Por que a proteção de dados é também uma questão de segurança da informação



PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO



TCU identifica riscos de segurança da informação em organizações públicas federais

A maioria dos índices avaliados apresenta nível de maturidade baixo ou intermediário de segurança. Fragilidades expõem instituições a ataques cibernéticos

Por Secom TCU
27/03/2024

RESUMO

- Auditoria avaliou a segurança da informação de organizações públicas federais
- Foram encontradas deficiências na configuração de controles recomendados pelas boas práticas para serviços de hospedagem web, e-mail e DNS (Domain Name Service)
- A maior parte das instituições estão expostas a ataques cibernéticos.
- Problemas são causados por falta de recursos ou investimento, de pessoal e de capacitação.

As principais causas da não implementação dos controles de segurança foram a **falta de recursos ou investimento, de pessoal e de capacitação**.









Segurança em risco: a ameaça crescente dos ataques de hackers a órgãos públicos

Cada vez mais comuns, eles evidenciam a necessidade de uma política de proteção

Por **Bruno Caniato**
Atualizado em 5 ago 2024, 09h54 - Publicado em 4 ago 2024, 08h00



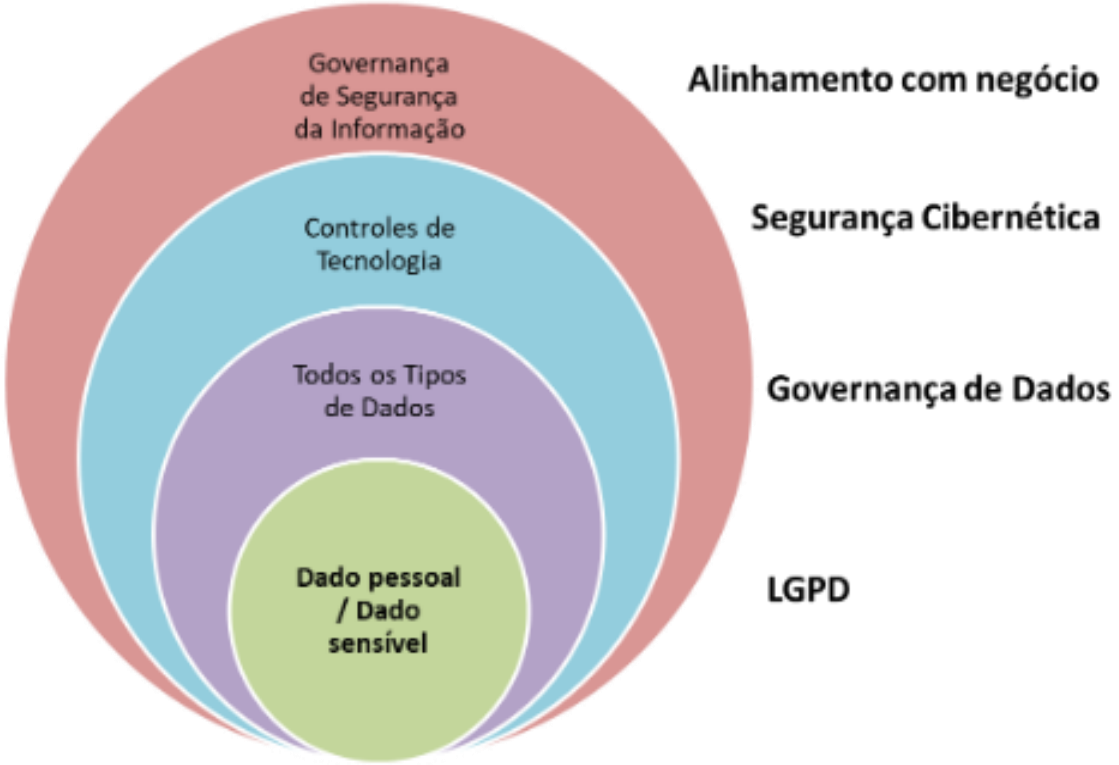
RISCOS AO TRATAR DADOS PESSOAIS





SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

De acordo com o art. 46 da LGPD, “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".



02

CLASSIFICAÇÃO DA INFORMAÇÃO

Só se protege adequadamente aquilo que se sabe classificar

LAI, art. 3º , IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

Lei 12.414/11 (Lei do Cadastro Positivo), art. 3, §3º

[...]

II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas; [...]

LGPD, art. 5º

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...]

NÍVEIS DE CLASSIFICAÇÃO DA INFORMAÇÃO

PÚBLICA

O que é

Sem restrição de acesso. A publicidade é a regra no setor público.

Exemplos

Editais, resultados de seleção, dados agregados de bolsas, currículos de agentes públicos.

Fundamento

CF, art. 5º, XXXIII; LAI, arts. 3º e 8º

PESSOAL

O que é

Identifica ou torna identificável uma pessoa natural. Acesso restrito a quem precisa e ao titular.

Exemplos

Nome com CPF, RG, endereço residencial.

Fundamento

LGPD, art. 5º, I; LAI, art. 31

PESSOAL SENSÍVEL

O que é

Dado pessoal com maior potencial discriminatório. Exige base legal do art. 11.

Exemplos

Saúde (atestados, laudos), raça/etnia em ações afirmativas, deficiência, biometria.

Fundamento

LGPD, arts. 5º, II, e 11

SIGILOSA

O que é

Classificada por autoridade (reservada 5, secreta 15, ultrassecreta 25 anos) ou protegida por sigilo legal.

Exemplos

Informações estratégicas; sigilo fiscal, bancário, industrial ou de pesquisa.

Fundamento

LAI, arts. 22 a 24

Regra prática: um arquivo assume o nível do dado mais protegido que contém. Uma planilha pública com uma coluna de CPF deixa de ser pública.

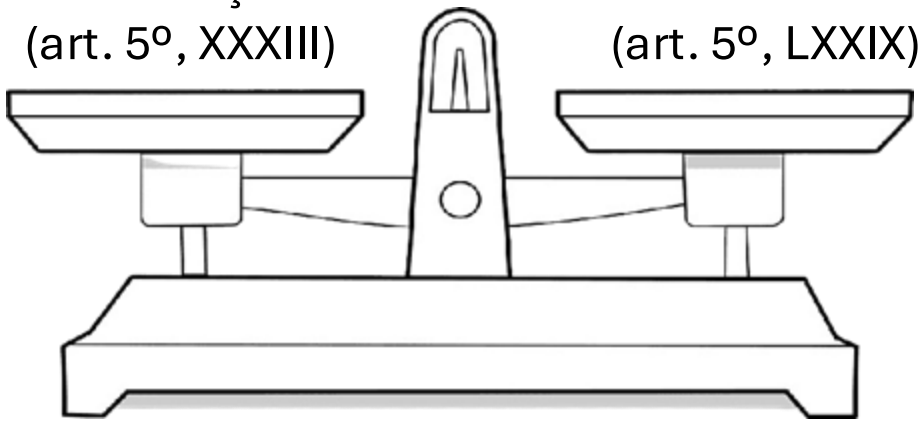
COMO TRATAR CADA NÍVEL NO DIA A DIA

1. Identifica alguém? → **2. É dado sensível?** → **3. Há sigilo legal?** → **4. Quem precisa?**

Nível	Onde armazenar	Como compartilhar	Quem acessa	Descarte
Pública	Portais e transparência ativa	Publicação aberta	Qualquer pessoa	Tabela de temporalidade
Pessoal	Sistemas e nuvem institucionais, pastas restritas	SEI, sistemas ou link nominal; nunca e-mail ou app pessoal	Somente quem precisa para a finalidade	Ao fim da finalidade (LGPD, arts. 15 e 16)
Pessoal sensível	Ambiente com acesso reforçado e criptografia	Só com base no art. 11; preferir dado anonimizado ou agregado	Grupo mínimo, com acessos registrados	Eliminação segura e registrada
Sigilosa	Sistemas próprios, com marcação do grau	Apenas a credenciados, com registro	Pessoas credenciadas (Decreto nº 7.845/2012)	Torna-se pública ao fim do prazo

CORRELAÇÕES E INTERSEÇÕES ENTRE LAI E LGPD

Acesso à Informação (art. 5º, XXXIII)



Direito de Dados (art. 5º, LXXIX)

Não aniquilamento do núcleo essencial

ESTRATÉGIAS PARA UMA GOVERNANÇA DE DADOS TRANSPARENTE, SEGURA E ÉTICA

Classificação e Avaliação das Informações

- Identifique e classifique os dados conforme a sensibilidade e o nível de risco.
- Distinga entre dados públicos, dados pessoais e dados sensíveis, aplicando diferentes critérios para divulgação, conforme a legislação.

Princípio da Minimização

- Divulgue apenas as informações estritamente necessárias para atender ao interesse público.
- Aplique técnicas de anonimização ou pseudonimização sempre que possível, para reduzir a exposição de dados pessoais.

Avaliação de Interesse Público

- Realize uma análise de interesse público antes de disponibilizar informações pessoais, ponderando entre o benefício da transparência e o direito à privacidade.
- Considere o impacto de divulgar dados pessoais, assegurando que o interesse público justifica sua publicação.

CUIDADOS NO TRATAMENTO DE DADOS PESSOAIS

A coleta deverá ocorrer apenas naquilo que for essencial para a atividade institucional, ou prestação do serviço requerido.

Quando usar a base legal o consentimento. Lembrar que o mesmo estipule com clareza a finalidade da coleta, os tratamentos que poderão ocorrer sobre os dados e a forma de solicitar a exclusão.



A coleta deverá ocorrer apenas naquilo que for essencial para a atividade institucional, ou prestação do serviço requerido.

Deve-se, ao máximo, evitar a recoleta de dados, ou seja, requerer dados que já estejam no poder da Instituição.

03

COMPARTILHAMENTO SEGURO DE DADOS

Finalidade, base legal, mínimo necessário
e canal adequado

ANTES DE COMPARTILHAR, RESPONDA A SEIS PERGUNTAS

1. Para quê?

A finalidade é específica e legítima? Finalidade genérica contraria a LGPD.

2. Com que base legal?

Qual hipótese do art. 7º (ou do art. 11, se houver dado sensível) autoriza o envio?

3. É o mínimo necessário?

O destinatário precisa de todos os campos? Dá para anonimizar ou agregar?

4. Para quem?

O destinatário está autorizado? Atua como controlador ou operador?

5. Por qual canal?

O meio é institucional, seguro e deixa registro?

6. Por quanto tempo?

Há prazo definido? O que acontece com os dados ao final?

Uma resposta "não sei" é sinal para parar e consultar o Encarregado pelo Tratamento de Dados Pessoais.

Compartilhamento de Dados

Público-Público

Art. 25. Os dados deverão ser mantidos em **formato interoperável** e estruturado **para o uso compartilhado**, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e **à disseminação e ao acesso das informações** pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de **execução de políticas públicas e atribuição legal pelos órgãos** e pelas entidades públicas, **respeitados os princípios** de proteção de dados pessoais elencados no art. 6º desta Lei.

Compartilhamento de Dados

Público-Privada

Art. 26.

§ 1º **É vedado** ao Poder Público transferir a entidades **privadas** dados pessoais constantes de bases de dados a que tenha acesso, **exceto**:

I - em casos de **execução descentralizada de atividade pública** que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;
III - nos casos em que os dados forem **acessíveis publicamente**, observadas as disposições desta Lei.
IV - quando houver **previsão legal** ou a transferência for respaldada em **contratos, convênios ou instrumentos congêneres**; ou
V - na hipótese de a transferência dos dados objetivar exclusivamente a **prevenção de fraudes e irregularidades**, ou proteger e **resguardar a segurança e a integridade do titular dos dados**, desde que vedado o tratamento para outras finalidades.

ACORDOS DE COMPARTILHAMENTO NA CAPES



Quando se aplica

Fluxo contínuo de compartilhamento entre a CAPES e outras instituições.

Apenas dados que não estão em transparência ativa: consulte antes os portais e bases da CAPES.

Antes do Acordo

Natureza jurídica do partícipe (pública ou privada sem fins lucrativos).

Bases legais: obrigação legal, políticas públicas ou órgão de pesquisa.

Particularidades: obrigações e responsabilidades de cada parte.

Governança

Processo único no SEI/CAPES como repositório de todas as solicitações.

Envio dos dados só após análise do Encarregado da CAPES.

Transparência ao titular (LGPD, arts. 6º, VI, e 23, I).

"Qualquer operação de compartilhamento de dados pessoais no âmbito da CAPES deve observar a forma indicada pela instituição e seguir as orientações do Encarregado pelo Tratamento de Dados Pessoais da CAPES."

Fonte: CAPES. Guia de Orientações: Acordos de Compartilhamento de Dados Pessoais. 1ª ed., out. 2025.

FORMULÁRIO DE COMPARTILHAMENTO DA CAPES

Agentes de tratamento

Controlador, operador ou cocontroladores, definidos a cada pedido. Cada parte indica seu Encarregado.

Base legal

Art. 7º, ou art. 11 se houver dado sensível. No art. 11, II, "b", a política pública deve ser instituída por lei ou regulamento. Transferência internacional: art. 33; crianças: art. 14.

Identificação e finalidade

Listar cada dado e destacar os sensíveis. Finalidade específica: descrição genérica contraria a LGPD (arts. 23 e 26).

Formato

Indicar o formato adequado (CSV, Excel, API). Recomenda-se oferecer mais de uma opção.

Duração do tratamento

Prazo expresso. Encerrada a finalidade, eliminação; conservação só nas hipóteses do art. 16.

Medidas de segurança

Art. 46: acesso rastreável, privilégio mínimo, protocolo seguro (OAuth2) via API, firewall, segmentação de rede e prevenção de intrusão.

Fonte: CAPES. Guia de Orientações: Acordos de Compartilhamento de Dados Pessoais, item 3. 1ª ed., out. 2025.

FLUXO DOS ACORDOS DE COMPARTILHAMENTO NA CAPES

01. Ofício

Envio do ofício de solicitação à Presidência da CAPES

02. Análise

Análise da demanda pelo Encarregado da CAPES

03. Acordo

Encarregado apresenta o modelo e inicia as negociações

04. Assinatura

Assinatura pela alta gestão de cada partícipe

05. Formulário

Envio do formulário de cada operação pelo Encarregado solicitante

06. Viabilidade técnica

Análise de cada operação pela área técnica

07. Registro

Registro do compartilhamento no processo SEI

Fonte: CAPES. Guia de Orientações: Acordos de Compartilhamento de Dados Pessoais, Anexo. 1ª ed., out. 2025.

CANAIS: O QUE USAR E O QUE EVITAR

USE

- Processo SEI para formalizar e registrar o compartilhamento
- Sistemas e APIs institucionais com autenticação (ex.: OAuth2)
- Nuvem corporativa com acesso nominal e data de expiração
- Arquivo criptografado, com a senha enviada por outro canal

EVITE

- WhatsApp e redes sociais para envio de dados pessoais
- Links "qualquer pessoa com o link", sem prazo
- Pen drive sem criptografia e impressões esquecidas na impressora
- Dados pessoais inseridos em ferramentas de IA não homologadas

04

NUVEM E ARMAZENAMENTO DIGITAL

A nuvem é segura quando é bem configurada e bem usada

NUVEM: A SEGURANÇA É COMPARTILHADA

VOCÊ E A INSTITUIÇÃO

- Classificação do que é enviado
- Quem tem acesso (permissões e links)
- Contas, senhas e MFA
- Cópias locais e downloads

PROVEDOR DE NUVEM

- Aplicação e disponibilidade do serviço
- Servidores, rede e armazenamento
- Data centers e segurança física

O ponto cego

O provedor protege a infraestrutura. O que se coloca na nuvem, quem acessa e como se compartilha é responsabilidade de quem usa.

Notícia • Estadão / TecMundo / Cibersegurança

AWS: Chaves de acesso vazadas dão controle total sobre contas corporativas na nuvem

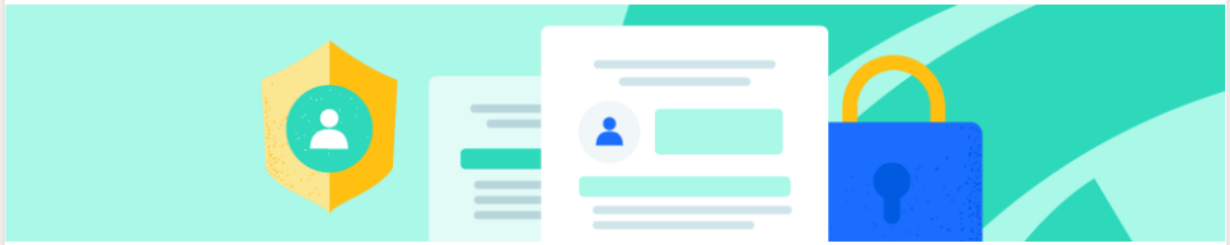
Mais de 9,3 mil credenciais da Amazon Web Services permanecem ativas na rede, a maioria sem renovação há cinco anos e com acesso irrestrito a sistemas empresariais

NUVEM: A SEGURANÇA É COMPARTILHADA

Docero Brasil

Entrar Menu

Política de privacidade do portal Doceru.com



A Política de Privacidade do Portal descreve a maneira pela qual o Administrador age sobre informações pessoais quando o Usuário usa os Serviços do Portal. Isso também se aplica a outras informações fornecidas ao usar o Portal. Os procedimentos de proteção de privacidade aplicados pelo Administrador são apresentados abaixo.

1. Informacje Osobiste

- **Przeglądanie Portalu.** Można oglądać zawartość **Portalu** bez **Konta Użytkownika**. Można też skontaktować się z **Administratorem** bezpośrednio przez wysłanie wiadomości e-mail w dziale **Kontakt**, nie rejestrując konta.
- **Konto w Portalu.**. Niektóre działania w Portalu, takie jak w szczególności zamieszczanie **Wpisów** na **Forum** i przesyłanie **Komentarzy** (a w nich **Linków** lub **Osadzonych Obiektów**) wymagają **Rejestracji Konta Użytkownika** i są możliwe wyłącznie dla **Zalogowanych Użytkowników** (Chyba że właściciel konta zezwala na aktywność Gości). Podczas **Rejestracji** należy wprowadzić pewne informacje osobiste, w tym adres e-mail i hasło. Są one używane w celu ochrony **Konta Użytkownika** przed **Nieautoryzowanym Dostępem**.
- **Informacje dotyczące użytkowania**. Podczas korzystania z **Portalu**, **Administrator** może rejestrować informacje na taki temat, jak (w szczególności):

ReclameAQUI Para você Para sua empresa Pesquise empresas

Home > Docero Brasil > ID 224449513

Não respondida

Dados pessoais expostos no site Doceru sem autorização

Docero Brasil → Rio de Janeiro - RJ 13/08/2025 às 15:17

MINISTÉRIO DA EDUCAÇÃO

GOVERNO DO BRASIL DO LADO DO POVO BRASILEIRO

BOAS PRÁTICAS COM NUVEM E ARMAZENAMENTO

Só conta institucional

Dados de trabalho não vão para drive pessoal.

Compartilhe com pessoas

Acesso nominal, não link aberto. Defina expiração.

Revise permissões

Retire o acesso de quem saiu do projeto ou do setor.

Ative o MFA

Senha vazada não basta para invadir a conta.

Organize por nível

Pastas separadas para dados pessoais e sensíveis.

Evite cópias soltas

Limpe downloads; pen drive só com criptografia.

Fonte única

Nada de bases paralelas em planilhas pessoais.

Elimine no prazo

Ao fim da finalidade, seguindo a temporalidade.

IA GENERATIVA TAMBÉM É NUVEM

1 em 5

organizações no mundo relatou violação ligada a "shadow AI" (uso de IA não autorizada)

87%

das organizações no Brasil não têm políticas de governança de IA

+R$ 591 mil

custo médio adicional de uma violação no Brasil associado a shadow AI

Regras de uso seguro

- Não insira dados pessoais, sigilosos ou código interno em ferramentas não homologadas.
- Use dados fictícios ou anonimizados nos comandos.
- Prefira as ferramentas contratadas pela instituição.
- Verifique se o histórico é usado para treinar o modelo.
- Revise o resultado: a IA também erra e inventa.

Fonte: IBM; Ponemon Institute. Cost of a Data Breach Report 2025 (dados globais e recorte Brasil).

CUIDADOS NO TRATAMENTO DE DADOS PESSOAIS



Feche sua sessão (logout) ao acessar sites que requeiram o uso de senhas, principalmente ao usar equipamentos compartilhados



Habilite autenticação em dois fatores



Cuidado ao digitar a sua senha com alguém por perto



Crie senhas fortes

CUIDADOS NO TRATAMENTO DE DADOS PESSOAIS

Evite usar a mesma senha para cadastro e acesso aos sistemas.

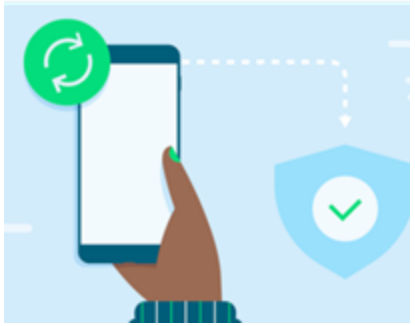


Nunca use dados pessoais ou sequências de teclado como senha

Caso desconfie que sua senha tenha sido descoberta, vazada ou usada em um equipamento invadido ou infectado, altere-a imediatamente

Tente mudar suas senhas regularmente, principalmente se acessar sistemas em dispositivos que são utilizados por várias pessoas.

CUIDADOS NO TRATAMENTO DE DADOS PESSOAIS



Mantenha sempre o sistema operacional e aplicativos instalados no seu equipamento com as atualizações mais recentes



Use apenas sistemas operacionais e programas originais.



Não saia clicando em links recebidos por meio de mensagens eletrônicas (SMS, e-mails, redes sociais, etc.). Desconfie sempre!

CUIDADOS NO TRATAMENTO DE DADOS PESSOAIS



Nunca forneça informações sensíveis em sites sem que você tenha solicitado o serviço que o exige, e o faça somente se confiar no site e se o mesmo estiver utilizando criptografia (procure pelo cadeado no navegador e um informativo de certificado digital).



Evite fazer cadastros em sites de venda desconhecidos pela Internet, especialmente fornecendo seus dados pessoais.



Cuidado ao vincular suas contas a aplicativos de terceiros.

05

CASOS REAIS DE EXPOSIÇÃO DE DADOS

Causas, impactos e lições aprendidas

MINISTÉRIO DA EDUCAÇÃO
GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

ATAQUES CIBERNÉTICOS

- **Mais de 30 mil estudantes de Alagoas** irão prestar o Enem em 2024. Para auxiliá-los, o governo estadual ofereceu uma plataforma de aprendizagem com material didático para o exame. Parece ótimo, só que não existe nenhum contrato que formalize o serviço e a relação entre o governo e a empresa.
- Pior: a empresa por trás da plataforma está – ou deveria estar – proibida de fazer negócios com o poder público.
- Assim, os dados de alunos e professores das séries finais do Ensino Médio – ou seja, adolescentes – e do Ensino de Jovens Adultos estão sendo cedidos a uma empresa sem nenhum tipo de transparência ou controle público.

GOVERNO DE ALAGOAS DESPEJA DADOS DE ALUNOS E PROFESSORES EM PLATAFORMA DE EMPRESA CONDENADA

Sem contrato, Secretaria de Educação oferece plataforma com material de apoio ao Enem. O pior: a empresa sequer poderia prestar serviços para o poder público.

ATAQUES CIBERNÉTICOS



Correio do Estado
https://correiodoestado.com.br › ... › Cidades › Polícia

Ataque hacker à UFGD e outras cinco universidades é alvo ...

Ataque hacker à UFGD e outras cinco **universidades** é alvo de operação da PF · Polícia Federal resgata estrangeiros em situação de trabalho escravo · MS tem a 4ª ...

Universidade Federal do Delta do Parnaíba UFDPar
https://ufdpar.edu.br › UFDPar › nota-sobre-o-ataque-h...

Nota sobre o ataque hacker sofrido pela UFDPar

12 de set. de 2023 — A **Universidade** Federal do Delta do Parnaíba (UFDPar) vem a público informar que, mediante a ameaça de um **ataque** cibernético publicado em um ...

Security Leaders
https://securityleaders.com.br › Artigos

Universidade Federal do Mato Grosso do Sul sofre ataque ...

O **ataque** cibernético foi diagnosticado no último domingo (24) por volta das 3 horas da madrugada pela equipe de cibersegurança da Agência de Tecnologia da ...

Correio Braziliense
https://www.correiobraziliense.com.br › Cidades DF

Palestra da UnB sofre ataque hacker com imagens de ...

4 de jul. de 2024 — Uma palestra on-line sobre cinema e gênero, promovida por professoras da **Universidade** de Brasília (UnB), teve de ser interrompida após um ...

A UFMS (Universidade Federal do Mato Grosso do Sul) sofreu um incidente de segurança em seus servidores que armazenam os sistemas institucionais e as senhas das contas de e-mails e drives institucionais.

4 CASOS, 4 LIÇÕES

Equifax
2017

Causa

Correção de segurança (Apache Struts) não aplicada por meses.

Impacto

Dados de cerca de 147 milhões de pessoas; acordo de até US$ 700 milhões (FTC, 2019).

Lição: Atualizar sistemas é medida de proteção de dados.

Capital One
2019

Causa

Firewall mal configurado em ambiente de nuvem (AWS).

Impacto

Cerca de 106 milhões de clientes afetados; multa de US$ 80 milhões (OCC, 2020).

Lição: Na nuvem, a configuração é de quem usa.

Power Apps
2021

Causa

Configuração padrão deixava listas de dados acessíveis ao público.

Impacto

38 milhões de registros expostos em 47 organizações, inclusive dados de vacinação.

Lição: Desconfie do padrão: revise antes de publicar.

Samsung
2023

Causa

Funcionários colaram código-fonte e notas de reunião no ChatGPT.

Impacto

Informação sigilosa enviada a terceiro; proibição interna de IA generativa.

Lição: IA pública equivale a compartilhamento externo.

Caso Smart Sampa



CNN BRASIL Nacional

Ao vivo Política Money WW Agro Infra

Nacional

Os novos links vazados reuniam em uma planilha de Excel, vídeos e acessos a câmeras de empresas privadas que colaboram com o monitoramento urbano da capital paulista.

Segundo reportagem do portal UOL, **a falha comprometeu o sigilo de 17 mil câmeras.**

A Prefeitura de São Paulo classificou a divulgação dos dados como "ato criminoso" e anunciou uma abertura de investigações, já a ANPD (Autoridade Nacional de Proteção de Dados) notificou o governo municipal cobrando explicações oficiais no prazo de cinco dias úteis.

Prefeitura diz à ANPD que 178 usuários do Smart Sampa tinham o mesmo padrão de senha

- Gestão Nunes reconhece acesso não autorizado e informa mudanças nos controles de segurança
- Em resposta à agência, município cita o reconhecimento facial obrigatório para acessar a plataforma

F DÊ UM CONTEÚDO 1

O QUE A ANPD TEM SANCIONADO NO SETOR PÚBLICO?

Órgão	Ano	Falha identificada	Sanção
Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo - IAMSPE	2023	Incidente não comunicado aos titulares; segurança inadequada	Advertência e comunicação aos titulares
Secretaria de Estado da Saúde-SC	2023	Exfiltração de cerca de 4 GB de dados de mais de 300 mil pessoas, sem comunicação individual	Quatro advertências e medidas corretivas
INSS	2024	Incidente não comunicado aos titulares; descumprimento de determinações	Publicização da infração por 60 dias
Secretaria de Estado de Educação do Distrito Federal	2024	Dados de saúde de mais de 3 mil crianças e adolescentes expostos; sem RIPD; comunicação 8 meses depois	Quatro advertências e medidas corretivas
Ministério da Saúde	2024	Comunicação tardia; monitoramento insuficiente; ausência de encarregado e de RIPD	Advertências e medidas corretivas



Padrão comum

Incidente seguido de silêncio.

Na maioria dos casos, a falta de comunicação aos titulares agravou a infração.

Fonte: decisões de fiscalização da ANPD, conforme compilação Confidata (2026). Conferir os processos oficiais antes de citar.

O QUE OS NÚMEROS MOSTRAM

R$ 7,19 mi

custo médio de uma violação de dados no Brasil em 2025 (+6,5% em um ano)

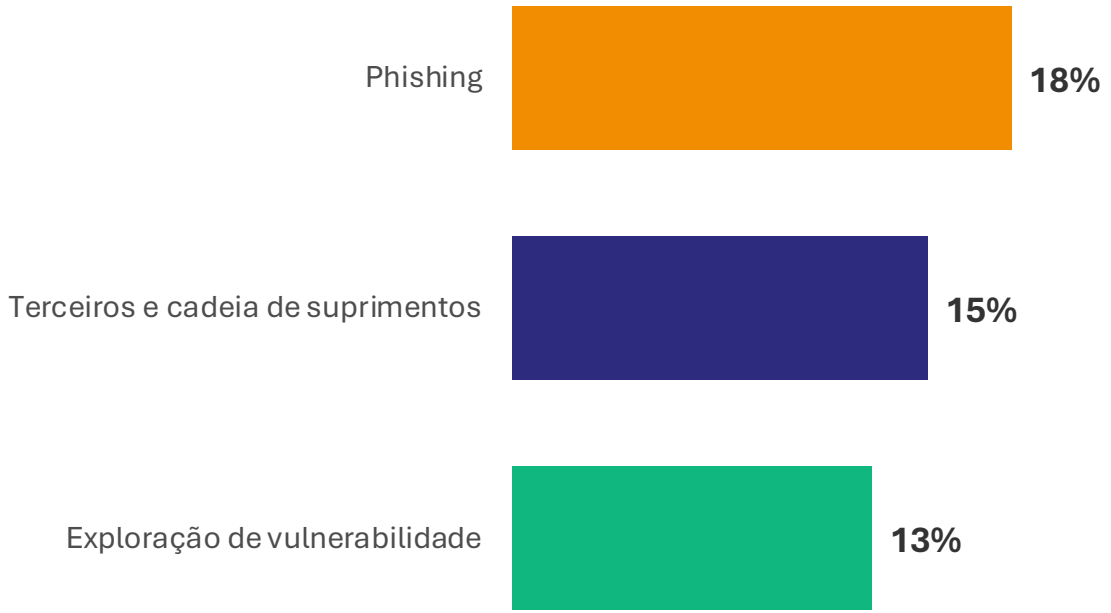
R$ 11,43 mi

custo médio no setor de saúde, o mais caro no país

241 dias

tempo médio global para identificar e conter uma violação

Principais vetores iniciais de ataque no Brasil (% das violações)



Fonte: IBM; Ponemon Institute. Cost of a Data Breach Report 2025 (600 organizações, mar./2024 a fev./2025).

MINISTÉRIO DA **EDUCAÇÃO**



gov.br/mec

MINISTÉRIO DA EDUCAÇÃO
ESPLANADA DOS MINISTÉRIOS, BLOCO L | BRASÍLIA DF | 70047-900
0800 616161