# Segurança na era Digital

## O que isso tem a ver com as Matrizes?

Marcele Sales Souza Bacelar
Jancarlos Menezes Lapa

**Livro do Estudante**

**Salvador**
**2024**

# Segurança na Era Digital
## O que isso tem a ver com Matrizes?

**AUTORES**
Msc. Marcele Sales Souza Bacelar
Currículo lattes:
http://lattes.cnpq.br/8388742064293455
E-mail: marcelecel@hotmail.com

Prof. Dr. Jancarlos Menezes Lapa
Currículo lattes:
http://lattes.cnpq.br/3502371499104482
E-mail: jancarloslapa@ifba.edu.br

**PROJETO GRÁFICO E EDITORAÇÃO**
Marcele Sales Souza Bacelar

**ORGANIZAÇÃO**
Marcele Sales Souza Bacelar | Jancarlos Menezes Lapa

**PESQUISA E REDAÇÃO**
Marcele Sales Souza Bacelar | Jancarlos Menezes Lapa

**REVISÃO**
Marcele Sales Souza Bacelar | Jancarlos Menezes Lapa

FICHA CATALOGRÁFICA ELABORADA PELO SISTEMA DE BIBLIOTECAS DO IFBA, COM OS DADOS FORNECIDOS PELO(A) AUTOR(A)

B116s Bacelar, Marcele Sales Souza

Segurança na era digital: o que isso tem a ver com as matrizes? / Marcele Sales Souza Bacelar; Jancarlos Menezes Lapa; -- Salvador, 2024.

30 p.

1. Matrizes. 2. Ensino médio integrado. 3. Educação profissional. 4. Matemática crítica. I. Lapa, Jancarlos Menezes, colab. II. TÍTULO.

CDU 377

# Ficha Técnica do Produto

**Origem:**
Programa de Pós-Graduação do Mestrado em Educação Profissional e Tecnológica do Instituto Federal de Ciência e Tecnologia da Bahia (IFBA)

**Nível a que se destina o produto:**
Nível Médio

**Área de Conhecimento:**
Ensino

**Público-alvo:** Estudantes do Ensino Médio

**Categoria deste Produto:**
Material didático instrucional (textual)

**Finalidade:**
Auxiliar estudantes e professores na promoção da formação omnilateral e emancipação, alinhando-se aos princípios da Educação Profissional e Tecnológica (EPT) e da Educação Matemática Crítica (EMC) como uma abordagem inovadora.

**Organização do Produto:**
Apresentação; Iniciando o diálogo: Problematizando; Organizando o conhecimento; Ampliando repertório: Aprofundando a Leitura; Estudo de Caso; e Refletindo Sobre: Aplicando conhecimentos.



**Idioma:** Português

**Cidade:** Salvador - Bahia

**Ano:** 2024

# Apresentação

Este e-book é parte integrante da proposta de ensino de Matemática para o Ensino Médio Integrado. Aborda o tema das Matrizes não apenas para transmitir conceitos matemáticos, mas também para conectar esses conceitos com questões relevantes da sociedade contemporânea, como a Segurança Digital.

Integrar temas atuais e pertinentes ao ensino de Matemática não só contextualiza o aprendizado, mas também o torna mais significativo para os estudantes, incentivando o protagonismo estudantil e a participação ativa na aprendizagem.

Ao utilizar situações-problema, busca-se promover o desenvolvimento de habilidades como análise crítica, interpretação e resolução de problemas, habilidades essenciais para os alunos se tornarem membros conscientes e engajados da sociedade. Além disso, ao enfatizar atividades individuais e coletivas, promove-se uma abordagem inclusiva que reconhece a diversidade de estilos de aprendizagem e incentiva a colaboração entre eles.

A ênfase na reflexão contínua e na capacidade de reavaliar e ajustar o próprio caminho de aprendizagem é fundamental para estimular a metacognição e a autoavaliação, habilidades que são valiosas não somente na Matemática, mas em todas as áreas da vida em sociedade.

Em resumo, oferecer uma abordagem educacional abrangente e centrada no estudante, que fomente o pensamento crítico, a conscientização social e o desenvolvimento de habilidades.

Aqui vamos problematizar, organizar conhecimento, ampliar repertório, aprofundar leituras e aplicar conhecimento por meio de atividades de produção individual e/ou coletivas, que nos faça refletir o percurso de aprendizagem sempre que necessário.

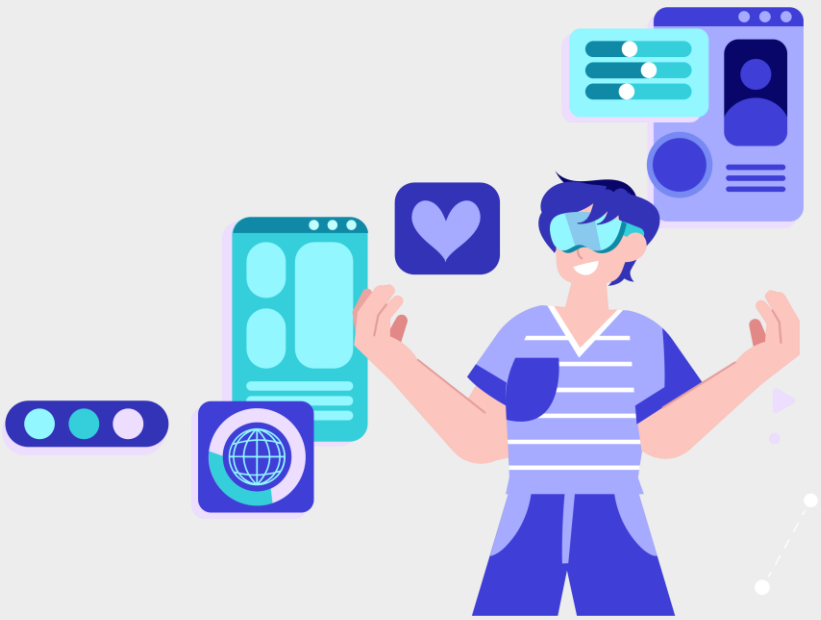
Vamos mergulhar nessa jornada?

Os Autores

# Sumário

# Sumário





# SEGURO?

**À medida que a sociedade se torna cada vez mais dependente da tecnologia e da internet, é essencial garantir a segurança de dispositivos e redes digitais, bem como proteger nossos dados pessoais de ataques cibernéticos. É importante adotar práticas de segurança, utilizar senhas fortes e criptografadas.**

# Iniciando o Diálogo...

## Problematizando

### Segurança digital e o vazamento de senhas

A notícia abaixo, publicada no *site* "Convergência Digital", nos traz um panorama, em números, sobre o vazamento de dados na internet no Brasil. Você já pensou sobre o impacto dessas informações na vida do cidadão comum? De acordo com as empresas que realizaram a pesquisa o Brasil teve 30,18 milhões de senhas vazadas.

Convergência Digital

Convergência Digital | Carreira | Cloud Computing | Internet Móvel | CDTV
Quem somos | Anuncie | Fale conosco | Newsletter
Gestão | Governo | Inclusão Digital | Inovação | Internet

SEGURANÇA

Trinta milhões de senhas foram vazadas no Brasil em 2022

Convergência Digital ... 08/05/2023 ... Convergência Digital

Em 2022, 30,18 milhões de senhas foram vazadas no país. É o que revela um levantamento feito pelo SafeLabs em parceria com a ISH, ambas empresas de cibersegurança do grupo ISH Tech.

O estado de São Paulo lidera a lista de incidentes, com 18.666.801 vazamentos, mais que o dobro do Rio de Janeiro (segundo colocado), com 9.237.689. Minas Gerais também ultrapassou a casa do milhão, com 1.122.777 incidentes.

O levantamento revela que o navegador que mais sofreu com roubo de informações armazenadas no Brasil foi o Google Chrome, com 3.909.813 credenciais vazadas. Em sequência estão o Microsoft Edge e Opera Browser, com 330.025 e 125.888 vazamentos, respectivamente.

Os dados apontam ainda que, logo atrás de Minas Gerais, estão os estados do Paraná, com 155.301 mil vazamentos, e o Rio grande do Sul, com 124.023. A Bahia ocupa o 6º lugar nesse ranking, com um total de 112,838 mil senhas vazadas.

**Atividade I**. Dialogando com o texto

1) De que se trata o texto apresentado?

2) É possível organizar as informações numéricas apresentadas em uma tabela? Se for possível, produza uma tabela com informações referentes ao quantitativo de dados vazados por estado, conforme mencionado no texto referente ao ano de 2022.

3) Qual é a quantidade de linhas e de colunas desta tabela?

4) Observando a tabela confeccionada por você, indique o maior valor inserido e o que esse número representa.

Produção Coletiva

5) Você sabe o que fazer para proteger seus dados de vazamentos e ataques cibernéticos? Junte-se com alguns colegas e elabore um infográfico contendo informações que auxiliem as pessoas na proteção de seus dados.

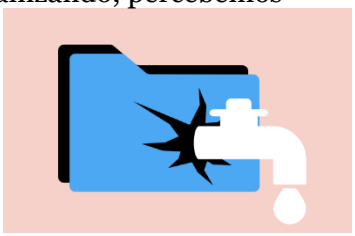
Dicas para começar a criação do seu primeiro infográfico:

1. Defina um objetivo claro.
2. Identifique o público-alvo.
3. Recolha a informação necessária.
4. Escolha o tipo de infográfico.
5. Adapte o conteúdo à sua ideia.
6. Escolha o tipo de estrutura.
7. Defina o *template* do seu infográfico.
8. Organize conteúdos e imagens da forma correta.
9. Escolha o meio físico ou virtual para confeccionar.
10. Partilhe o infográfico com o seu público-alvo.


Fonte: https://www.growunder.com/images/blog/Como-fazer-um-infografico.jpg

# Organizando o conhecimento

Retomando as informações anteriores sobre o vazamento de senhas e organizando, percebemos um *ranking* que contempla os estados que ocupam do 1º ao 6º lugar. Vejamos:



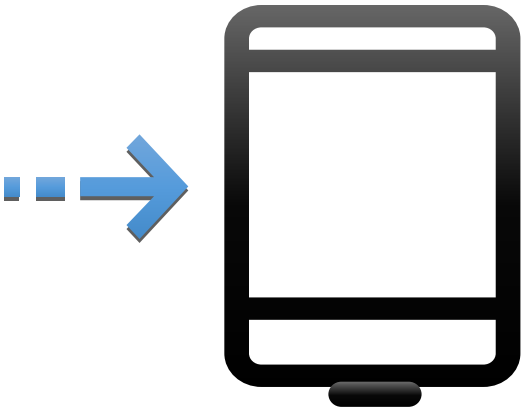
| Estados | Quantitativo de senhas vazadas |
|---|---|
| São Paulo | 18.666.801 |
| Rio de Janeiro | 9.237.689 |
| Minas Gerais | 1.122.777 |
| Paraná | 155.301 |
| Rio Grande do Sul | 124.023 |
| Bahia | 112.838 |

Fonte:https://www.convergenciadigital.com.br/Seguranca/Trinta-milhoes-de-senhas-foram-vazadas-no-Brasil-em-2022-63146.html

Você observou a maneira como os dados acima foram organizados e apresentados? Isso mesmo! Eles estão organizados numa tabela, pois, é uma forma de facilitar a leitura e a interpretação dessas informações. Podemos simplificar ainda mais apresentando apenas os dados numéricos dispostos em filas verticais e filas horizontais.

Essas informações numéricas podem ser representadas de outra maneira, utilizando o conceito de MATRIZES. Assim, teremos:

| Estados | Quantitativo de senhas vazadas |
|---|---|
| São Paulo | 18.666.801 |
| Rio de Janeiro | 9.237.689 |
| Minas Gerais | 1.122.777 |
| Paraná | 155.301 |
| Rio Grande do Sul | 124.023 |
| Bahia | 112.838 |



Tabelas com $\boldsymbol{m}$ linhas e $\boldsymbol{n}$ colunas ($m$ e $n$ números naturais diferentes de zero), como essa, são denominadas matrizes $\boldsymbol{m}$ x $\boldsymbol{n}$. Na tabela anterior, temos, portanto, uma matriz 6 x 1, lê-se “seis por um”. Utilizamos parênteses ( ), entre colchetes [ ] ou entre barras duplas|| ||, para representar as matrizes. Genericamente, representamos uma matriz **A** do tipo *mxn*, escrevendo de forma abreviada $A = (a_{ij})_{mxn}$ ou simplesmente $A = (a_{ij})$

$$A_{mxn} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix} \quad \text{com } \boldsymbol{m}, \boldsymbol{n} \in \mathbb{N}^*$$

A teoria das matrizes foi criada no século XIX pelo matemático e astrônomo inglês Arthur Cayley (1821 – 1895) e tem uma vasta aplicação na Física, Computação Gráfica, Engenharia, Administração e na Matemática.

Mas, você pode estar se perguntando o que a Matemática e as matrizes têm a ver com a segurança de dados? As Matrizes são utilizadas no campo da tecnologia, seja na programação ou na computação gráfica, por meio de animações.

# Ampliando repertório...

## Aprofundando a leitura

**Texto II**

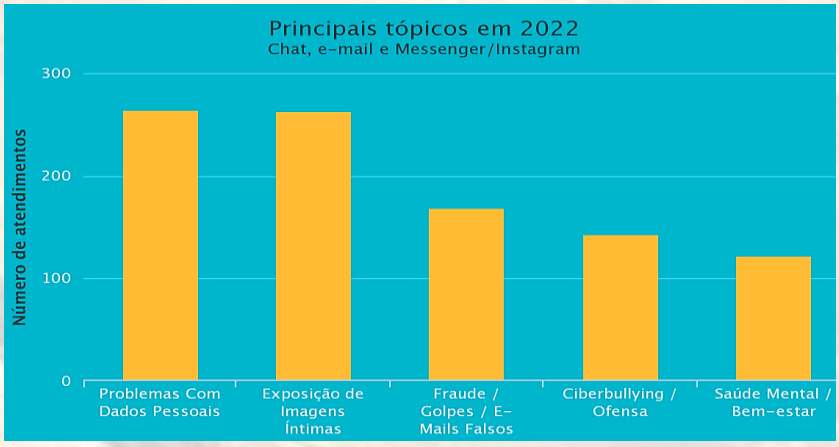
### Segurança digital e a infinidade de dados que compartilhamos na web

Fonte: https://new.safernet.org.br/content/seguran%C3%A7a-digital#mobile

A segurança nos ambientes digitais apresenta-se como um desafio complexo. Podemos pensar em diferentes tipos e níveis de segurança - das preocupações com segurança nacional à proteção da senha pessoal no celular. Na sociedade da informação, proteger e cuidar desses dados é uma tarefa para todos. A internet é também um ambiente de produtos que são trocados, vendidos e negociados. Quando lembramos que a Internet das Coisas já é uma realidade, conectando não apenas pessoas, mas bilhões de objetos como redes, o desafio de conectar-se com segurança exige cada vez mais atenção.

O assunto também envolve cuidado com dados pessoais que deixamos em sites como redes sociais, de busca, nos milhões de e-mails e mensagens, sites de compras, nos programas de fidelidade, nos cartões de crédito e nos dispositivos móveis que concentram cada vez mais informações detalhadas sobre nossas vidas. Nunca pensamos a segurança como oposto de liberdade, mas como condição para que as liberdades das diferentes pessoas sejam respeitadas nos diferentes contextos nos quais nos relacionamos dentro e fora da rede.

Considerando o direito à segurança da informação como um dos direitos humanos que defendemos também na rede, a SaferNet oferece algumas dicas para preservar os direitos de proteção contra abusos e violações de privacidade ou das liberdades de expressão, e posicionamento sexual, religioso, político e de pensamento. O desafio é imenso, mas trabalhamos na construção de plataformas de informações para despertar a consciência dos internautas sobre a importância de saber fazer boas escolhas nos cliques diários na Internet.




**SaferNet**

A SaferNet é uma organização não governamental, sem fins lucrativos, que reúne cientistas da computação, professores, pesquisadores e bacharéis em direito com a missão de defender e promover os direitos humanos na Internet.

O texto acima nos chama a atenção para a importância das escolhas que fazemos na internet e sobre o cuidado com a segurança digital. Em sua página *web*, a SaferNet, disponibiliza dados sobre os atendimentos realizados aos internautas, divididos por indicadores de *hotline* (atendimento rápido) e *helpline* (linha de apoio). Este último é um serviço de orientação sobre crimes e violações dos Direitos Humanos na internet. A SaferNet, em seu canal de ajuda e orientação, auxiliou 36.609 pessoas nas 27 unidades da federação, atendeu 9.739 crianças e adolescentes, 2.503 pais e educadores, 4.737 jovens e 19.630 outros adultos.


Observem na tabela abaixo, os dados de atendimentos levantados pela SaferNet referentes aos anos de 2019 a 2022, sobre as principais violações para as quais os internautas brasileiros pedem ajuda.

**Número de atendimentos por tópicos - Helpline ( 2019 - 2022)**

| Tópicos \ Ano | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|
| Problemas com dados pessoais | 340 | 232 | 339 | 261 |
| Exposição de imagens íntimas | 466 | 354 | 273 | 253 |
| Fraude/ Golpes/ E-mails falsos | 227 | 187 | 211 | 168 |
| Ciberbullying/Ofensa | 341 | 232 | 188 | 137 |

Fonte: https://indicadores.safernet.org.br/helpline/helplineviz/helpchart-page.html#

Vamos escrever a matriz associada a essa tabela e identificar a sua ordem? Essa escrita é feita observando apenas os dados numéricos, vejamos:

$$T = \begin{pmatrix} 340 & 232 & 339 & 261 \\ 466 & 354 & 273 & 253 \\ 227 & 187 & 211 & 168 \\ 341 & 232 & 188 & 137 \end{pmatrix}_{4 \times 4}$$

Essa matriz possui 4 linhas e 4 colunas, logo é uma matriz do tipo 4 x 4, lê-se “quatro por quatro”. Quando as matrizes têm o número de linhas igual ao número de colunas, denominamos de **Matriz Quadrada**; neste caso, é uma matriz quadrada de ordem 4.

Algumas matrizes são chamadas de especiais, por terem um papel de destaque decorrente de apresentar certas características, a exemplo da matriz quadrada, a matriz identidade e a matriz nula.

Em toda matriz quadrada tipo $n$ x $n$ existem duas diagonais: a Diagonal Principal e Diagonal Secundária. A diagonal principal contém elementos $\mathbf{a_{ij}}$ em que $\mathbf{i = j}$, ou seja, $\mathbf{\{a_{ij} | \ i = j\} = \{a_{11}, a_{22}, a_{33}, \ldots, a_{nn}\}}$. Os elementos $\mathbf{a_{ij}}$ cuja soma dos índices é igual a $\boldsymbol{n + 1}$, formam a diagonal secundária.

$$A_{3x3} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Diagonal Secundária

Diagonal Principal

**Matriz Identidade** é a matriz quadrada em que os elementos da diagonal principal são iguais a 1 e os demais, iguais a zero, indicamos por $I_n$. A **Matriz Nula** tem todos os elementos iguais a zero. Sendo a matriz nula, quadrada de ordem n, indicaremos por $0_n$.

Matriz Identidade

$$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Matriz Nula

$$F = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}_{4x3}$$


# Refletindo sobre...

## Aplicando conhecimentos

1) A partir da leitura e da sua observação como usuário da rede, o compartilhamento de dados na utilização de sites beneficia ou prejudica o usuário? Você considera que está correndo riscos? Em quais situações? Justifique o seu posicionamento apresentando um exemplo.

2) O Painel *Helpline* nos traz informações de atendimentos feito pela SaferNet, no período compreendido entre 2007 e 2022, em 27 unidades da federação. Represente, se possível, por meio de uma tabela e apresente a matriz associada, indicando a sua ordem.

3) No texto da página anterior, temos como exemplo a matriz T, em que seus elementos são números de atendimentos *helpline* por tópicos, quais elementos dessa matriz pertencem a diagonal principal?

4) Fazendo a leitura da tabela com o número de atendimentos da SaferNet, você acredita que exista um órgão governamental responsável exclusivamente para cuidar de questões relacionadas a crimes virtuais, vazamentos de dados, fraudes e que oriente e auxilie pessoas que passaram por estas situações?

Socializando Informações

5) De acordo com o texto da SaferNet, a ONG considera "*o direito à segurança da informação como um dos direitos humanos que defendemos também na rede...*". O direito é sempre assegurado por lei. Você conhece ou já ouviu falar em "Marco Civil da Internet" e o que apresenta sobre a segurança da informação?

Caso não conheça busque e apresente as suas impressões através de um *podcast*.

Dicas para produção do *podcast*:


# Iniciando o Diálogo...

## Problematizando

**Texto III**

### Segurança de dados na WEB: Como se proteger?

A internet se tornou uma ferramenta indispensável no nosso cotidiano; porém, junto a ela vem a preocupação com a segurança dos nossos dados. Você já se deu conta da quantidade de informações pessoais que compartilhamos diariamente? Desde informações de *login* em contas de redes sociais, Wi-Fi e e-mails até dados bancários e transações comerciais, tudo isso pode estar em risco sem as medidas de segurança adequadas. Já imaginou o que pode acontecer conosco tendo dados expostos? Então, como podemos nos proteger?

Uma das formas de nos proteger é utilizando senhas fortes e seguras, pois através delas podemos manter nossos dados pessoais seguros. Não dá para escolher como senha a palavra "senha" e achar que seus dados estão seguros, concordam? O fortalecimento da senha é uma barreira vital inicial. Além disso, é recomendado optar pela autenticação em dois fatores, proporcionando uma segurança adicional, e complementar com a utilização de gerenciadores de senhas.

Na pesquisa realizada anualmente, em 30 países incluindo o Brasil, por uma empresa especializada, mostra que as pessoas ainda utilizam senhas fracas para proteger suas contas. Esta cultura afeta as senhas, que se tornam vulneráveis e sem grau de dificuldade para serem quebradas, tendo o invasor êxito em menos de 1 segundo. Veja na tabela o *ranking* com base em 2022.

**Quantitativo mundial de senhas mais comuns por ano**

| Classificação 2022 | Ano / Senhas | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| 1 | senha | 830.846 | 360.467 | 20.958.297 | 4.929.113 |
| 2 | 123456 | 2.485.216 | 2.543.285 | 103.170.552 | 1.523.537 |
| 3 | 123456789 | 1.052.268 | 961.435 | 46.027.530 | 413.056 |
| 4 | convidado | 0 | 0 | 0 | 376.417 |
| 5 | qwerty | 348.762 | 156.765 | 22.317.280 | 309.679 |

**Fonte: NordPass**

**Padrões em composição de senhas**

O *ranking* de piores senhas muda todos os anos, mas a previsibilidade do ser humano na manutenção de alguns hábitos faz com que seja possível perceber a permanência de padrões na composição de senhas, como o uso de nomes de filmes, personagens, times de equipes esportivas e até alimentos.


Fonte: https://s1.npass.app/nordpass/media/1.1868.0/images/web/top-worst-passwords/all-time-favourite-image.web


Nas tabelas a seguir, são apresentadas informações sobre o número de senhas ou *password* mais comuns no Brasil e no mundo, de acordo com o modelo de senha escolhido, nos anos de 2021 e 2022.

**Quantitativo de senhas mais comuns em 2021**

| Senhas / Local | senha | 123456 | 123456789 |
|---|---|---|---|
| **Brasil** | 103500 | 1003925 | 326815 |
| **Mundo** | 20.958.297 | 103.170.552 | 46.027.530 |

**Quantitativo de senhas mais comuns em 2022**

| Senhas / Local | senha | 123456 | 123456789 |
|---|---|---|---|
| **Brasil** | 541 | 13099 | 4237 |
| **Mundo** | 4.929.113 | 1.523.537 | 413.056 |

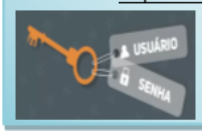
Observamos com as tabelas que o quantitativo das três senhas mais comuns no Brasil e no mundo apresenta variação de valores de 2021 para 2022. Isto pode indicar que as pessoas não consideram importante criar "boas" senhas ou estão colocando a proteção de seus dados em segundo plano.

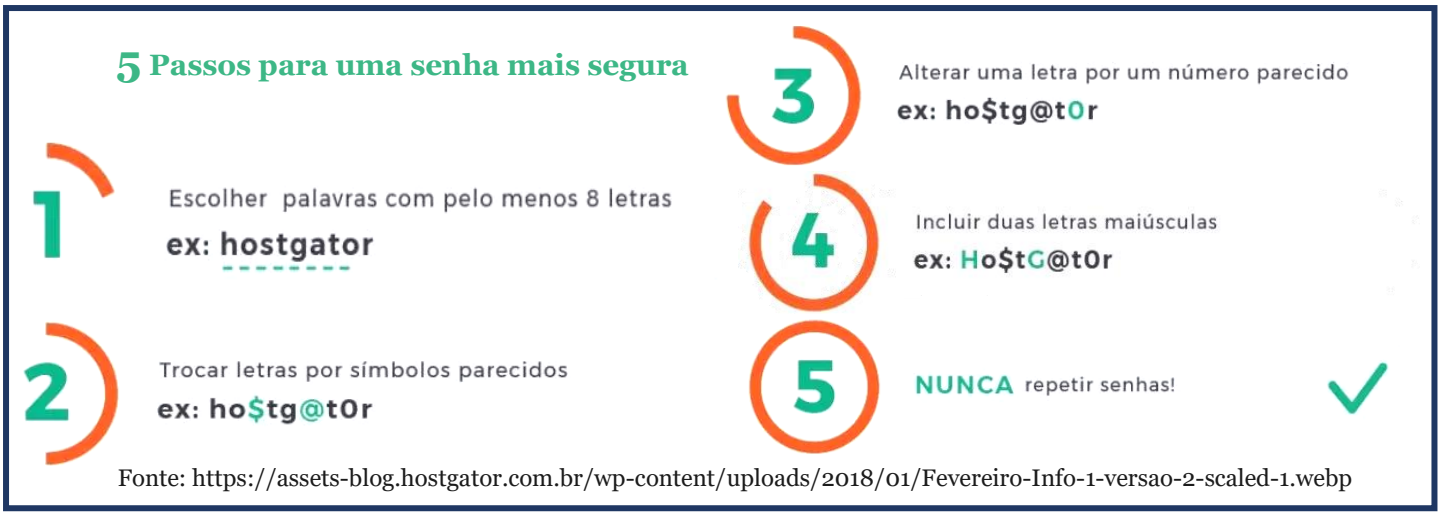
Na composição de senhas, o ideal é não optar por composições tão óbvias, preferir utilizar simultaneamente letras maiúsculas, minúsculas e caracteres especiais, além de inserir números. Outra informação valiosa é não utilizar senhas iguais para acessar diferentes plataformas onde você tem cadastro, caso isso ocorra você irá transformar uma senha, por mais forte que seja no momento da sua criação, em uma senha vulnerável.

***Você Sabia ?***
***Dia Mundial da Senha!***

Toda primeira quinta-feira de maio é conhecido internacionalmente como o **Dia Mundial da Senha.** A "comemoração" existe desde 2013, idealizada pelo pesquisador de Segurança da Informação Mark Burnett e posteriormente adotada pela Intel como um lembrete para os usuários reforçarem a segurança com seus dados.

Fonte: https://centralti.com.br/dia-mundial-da-senha-voce-sabia/




Fonte: https://assets-blog.hostgator.com.br/wp-content/uploads/2018/01/Fevereiro-Info-1-versao-2-scaled-1.webp

**Atividade II**. Dialogando com o texto

1) De que maneira podemos determinar o quantitativo total de cada senha comum mais utilizadas, no Brasil e no mundo, ao final desses dois anos?

2) Represente, na forma matricial, as tabelas referentes ao vazamento de senhas dos anos de 2021 e 2022. Indique também a ordem de cada uma das matrizes representadas.

3) Qual o quantitativo total de cada senha mais comum utilizadas, no Brasil e no mundo, ao final desses dois anos?

4) Qual a ordem da matriz obtida no item 3?

5) Identifique quais são os elementos $a_{11}$, $a_{21}$, $a_{13}$ dessa matriz e o que eles representam.

6) Encontre o aumento ou redução no quantitativo das senhas "123456" e "123456789", no ano de 2022 em relação ao ano de 2021 e escreva na forma matricial.

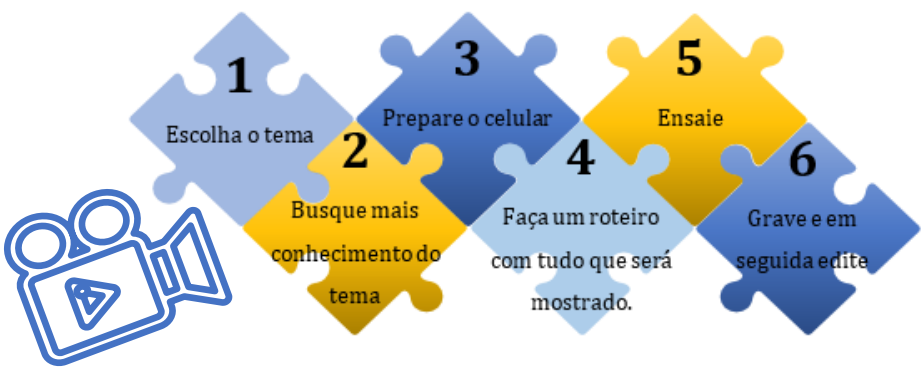
7) O que se pode constatar no ano de 2022? Ocorreu um aumento ou redução no quantitativo de senhas do Brasil e do mundo em relação ao ano de 2021? Justifique.

8) Considere o seguinte cenário, por um motivo desconhecido as análises referentes as senhas mais utilizadas em 2023 mostraram que se mantiveram no topo do *ranking* as mesmas senhas de 2022 e seu quantitativo foi quadruplicado. Represente os dados de 2023 numa tabela e em seguida em sua forma matricial.

Produção Coletiva

9) As tabelas anteriores nos dão um panorama de como os usuários brasileiros não criam "boas senhas" para suas redes sociais, e-mails, etc. Agora que você já sabe os tipos de senhas que **não** devemos utilizar, por nos tornar vulneráveis a ataques cibernéticos, produza um vídeo sobre como criar ou escolher senhas fortes para proteger suas contas e informações. Para criar o vídeo siga as dicas abaixo.

Dicas para produção do vídeo:




# Organizando o conhecimento

As duas matrizes que você escreveu, correspondentes a cada tabela, podem ser representadas pelas letras A e B. Intuitivamente, sabemos que vamos somar as quantidades de cada senha adicionando os elementos correspondentes. Este resultado pode ser representado pela matriz C, ou seja, $A_{2x3} + B_{2x3} = C_{2x3}$, em que cada elemento $c_{ij} = a_{ij} + b_{ij}$, para $1 \leq i \leq m$ e $1 \leq j \leq n$. Temos assim, a soma de duas matrizes de mesma ordem. Vejamos:

$$A + B = \begin{pmatrix} 103500 & 1003925 & 326815 \\ 20958297 & 103170552 & 46027530 \end{pmatrix} + \begin{pmatrix} 541 & 13099 & 4237 \\ 4929113 & 1523537 & 413056 \end{pmatrix} =$$

$$\begin{pmatrix} 103500+541 & 1003925+13099 & 326815+4237 \\ 20958297+4929113 & 103170552+1523537 & 46027530+413056 \end{pmatrix} = \begin{pmatrix} 104041 & 1017024 & 331052 \\ 25887410 & 104694089 & 46440586 \end{pmatrix} = C$$

Além da adição, é possível realizar outras operações envolvendo as matrizes, tais como subtração (representa pela soma com a oposta), multiplicação de matrizes e de número (escalar) por matriz. No item 6, por exemplo, da atividade anterior, para encontrar o aumento ou redução no quantitativo de senhas "123456" e "123456789", utilizamos operações que, na forma matricial, representa a subtração de matrizes.

| Quantitativo de senhas mais comuns em 2021 | | |
|---|---|---|
| Senhas / Local | 123456 | 123456789 |
| Brasil | 1003925 | 326815 |
| Mundo | 103.170.552 | 46.027.530 |

| Quantitativo de senhas mais comuns em 2022 | | |
|---|---|---|
| Senhas / Local | 123456 | 123456789 |
| Brasil | 13099 | 4237 |
| Mundo | 1.523.537 | 413.056 |

Fazendo a análise comparativa do quantitativo de cada senha nos anos de 2021 e 2022, verifica-se mudança nos valores que indicam redução. Para precisar o quanto foi reduzido em relação às senhas "123456" e "123456789", recorremos à subtração, conforme a tabela a seguir.

| Aumento ou redução 2022-2021 | | |
|---|---|---|
| Senhas / Local | 123456 | 123456789 |
| Brasil | 13099 - 1003925 | 4237 - 326815 |
| Mundo | 1.523.537- 103.170.552 | 413.056 - 46.027.530 |

Utilizando a ideia de matriz, semelhante ao que foi realizado com a operação de adição, escrevemos as matrizes "E", referente ao quantitativo de senhas de 2021, e "F", referente ao quantitativo de 2022, obtendo a diferença. A diferença de matrizes é realizada fazendo a soma da primeira com a oposta da segunda matriz. Este resultado pode ser representado pela matriz G, ou seja, $F_{2x2} - E_{2x2} = G_{2x2}$ em que cada elemento $g_{ij} = f_{ij} - e_{ij}$, para $1 \leq i \leq m$ e $1 \leq j \leq n$. Assim, temos a subtração de duas matrizes de mesma ordem.

$$F - E = \begin{pmatrix} 13099 & 4237 \\ 1523537 & 413056 \end{pmatrix} - \begin{pmatrix} 1003925 & 326815 \\ 103170552 & 46027530 \end{pmatrix} = \begin{pmatrix} 13099 & 4237 \\ 1523537 & 413056 \end{pmatrix} + \begin{pmatrix} -1003925 & -326815 \\ -103170552 & -46027530 \end{pmatrix} =$$

$$\begin{pmatrix} 13099+(-1003925) & 4237+(-326815) \\ 1523537+(-103170552) & 413056+(-46027530) \end{pmatrix} = \begin{pmatrix} -990826 & -322578 \\ -101647015 & -45614474 \end{pmatrix} = G$$

Outra operação bastante realizada é a multiplicação de número por matriz, também chamada de multiplicação por escalar. Observando o item 8, que apresenta a situação hipotética de ter o quantitativo de senhas quadruplicado em 2023, verifica-se que para encontrar este quantitativo basta multiplicar os dados da tabela de 2022 pelo número quatro, vejamos:

| Quantitativo de senhas mais comuns em 2023 | | |
|---|---|---|
| Senhas / Local | 123456 | 123456789 |
| Brasil | 4. (13099) | 4. (4237) |
| Mundo | 4. (1.523.537) | 4. (413.056) |

Escrevendo na notação de matrizes, temos:

$$4.F = 4 \cdot \begin{pmatrix} 13099 & 4237 \\ 1523537 & 413056 \end{pmatrix} = \begin{pmatrix} 52396 & 16948 \\ 6094148 & 1652224 \end{pmatrix}$$

Não podemos deixar de mencionar a operação de multiplicação entre matrizes. Acompanhe a situação a seguir:

Uma empresa de segurança cibernética detectou vazamentos de senha em três contas de seus usuários. A complexidade da senha representa sua força e isso vai determinar quanto tempo o criminoso vai levar para descobri-la, onde valores altos indicam senhas mais difíceis de serem quebradas. Além disso, a empresa possui uma lista de técnicas de quebra de senha, cada uma associada a um tempo estimado necessário para quebrar uma senha. Observe as tabelas a seguir:

Qual é o tempo mínimo (em segundos) necessário para quebrar cada uma das três senhas usando as três técnicas observadas pela empresa?

| Força da Senha | | | |
|---|---|---|---|
| Técnica / Senhas | T1 | T2 | T 3 |
| P@ssw0rd | 5 | 7 | 4 |
| s3Curity | 6 | 5 | 3 |
| 123456 | 1 | 2 | 1 |

| Tempo de quebra da técnica(s) | |
|---|---|
| T1 | 3 |
| T2 | 6 |
| T3 | 10 |

Para determinar o tempo mínimo de quebra de cada senha em cada uma das três técnicas, fazemos os seguintes cálculos: **P@ssword**: 5. 3 + 7. 6 + 4. 10 = 15 +42 + 40 = 97 → 97 segundos

**s3Curity**: 6. 3 + 5. 6 + 3. 10 = 18 +30 + 40 = 78 → 78 segundos

**123456**: 1. 3 + 2. 6 + 1. 10 = 3 +12 + 10 = 25 → 25 segundos

Esse cálculo pode ser feito utilizando as matrizes. Considere a matriz T, de ordem 3x1, que fornece o tempo mínimo (em segundos) de quebra de senha para as três técnicas observadas, e a matriz S, de ordem 3x3, que fornece a quantidade de tempo (em segundos) de quebra de cada senha para os três usuários.

$$T = \begin{matrix} \text{Tempo} \\ \begin{bmatrix} 3 \\ 6 \\ 10 \end{bmatrix} \end{matrix} \begin{matrix} \\ \rightarrow \text{Téc. 1} \\ \rightarrow \text{Téc. 2} \\ \rightarrow \text{Téc. 3} \end{matrix} \quad \text{e} \quad S = \begin{matrix} T_1 & T_2 & T_3 \\ \begin{bmatrix} 5 & 7 & 4 \\ 6 & 5 & 3 \\ 1 & 2 & 1 \end{bmatrix} \end{matrix} \begin{matrix} \rightarrow \text{P@ssword} \\ \rightarrow \text{s3Curity} \\ \rightarrow 123456 \end{matrix}$$

Vejamos como obter a matriz M = S.T, sendo M a matriz que mostra o tempo mínimo de quebra de cada uma das senhas pelas três técnicas.

$$S \cdot T = \begin{pmatrix} 5 & 7 & 4 \\ 6 & 5 & 3 \\ 1 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 6 \\ 10 \end{pmatrix} = \begin{pmatrix} 5 \cdot 3 + 7 \cdot 6 + 4 \cdot 10 \\ 6 \cdot 3 + 5 \cdot 6 + 3 \cdot 10 \\ 1 \cdot 3 + 2 \cdot 6 + 1 \cdot 10 \end{pmatrix} = \begin{pmatrix} 97 \\ 78 \\ 25 \end{pmatrix} = M$$

Para saber mais sobre as operações com matrizes acesse o QR Code.

SCAN ME

Generalizando, temos:

$s_{11}.t_{11}+s_{12}.t_{21}+s_{13}.t_{31} = m_{11}$; $s_{21}.t_{11}+s_{22}.t_{21}+s_{23}.t_{31} = m_{21}$; $s_{31}.t_{11}+ s_{32}.t_{21}+s_{33}.t_{31} = m_{31}$. Ou seja, o produto de duas matrizes é a soma dos produtos dos elementos da i-ésima linha de S pelos elementos correspondentes da j-ésima coluna de T. Para realizar o produto, é necessário que a quantidade de colunas de S seja igual ao número de linhas de T.

# Ampliando repertório...

# Vejamos algumas notícias sobre o tema

g1 TECNOLOGIA

fique por dentro Lucro do FGTS Caneta

## Vazamento de dados pessoais: veja como se proteger e o que fazer se for vítima

Especialistas explicam como descobrir se seus dados vazaram, fraudes com seu nome e os meios para evitar golpes.

Por g1
08/05/2023 15h14 · Atualizado há 2 meses

veja

Política

## Governo silencia sobre a violação da segurança nacional

Sem explicações oficiais proliferam versões convergentes num ponto: invasores conseguiram acesso a toda rede da administração pública federal.

Por José Casado
Atualizado em 4 ago 2023, 12h02 - Publicado em 27 dez 2021, 08h00

veja

Mundo

## Hackers chineses invadiram e-mails do governo dos EUA, diz Microsoft

Ação teria afetado tanto agências federais como outras 25 organizações e faria parte de uma campanha de espionagem iniciada em maio deste ano

Por Da Redação
Atualizado em 12 jul 2023, 18h52 - Publicado em 12 jul 2023, 17h19

g1 RONDÔNIA

## Rondônia registra 17 mil casos de senhas vazadas em 2022; especialista em smartphones alerta sobre segurança na rede

De acordo com Paulo Roberto, expert em telefonia, as pessoas expostas na internet devem se proteger e dificultar o trabalho dos hackers

Por g1 RO
04/07/2023 10h37 · Atualizado há 2 meses


**Você sabia?**

Os ataques de *phishing* são uma forma comum de tentativa de obtenção de informações pessoais. Os *cibercriminosos* enviam e-mails ou mensagens falsas, fingindo serem entidades confiáveis, para induzir as pessoas a fornecerem informações confidenciais, como senhas e números de cartão de crédito.

# Estudo de Caso

Acompanhe no texto a seguir o que aconteceu com a Sra. Regina, esta matéria foi publicada no jornal folha de São Paulo em setembro de 2022.

A aposentada Regina Silva, 66, moradora da zona sul de São Paulo, é um exemplo. Sem saber como uma instituição financeira conseguiu suas informações pessoais, tornou-se vítima do uso não autorizado de seus dados, quando uma linha de crédito apareceu em sua conta sem que ela soubesse a origem. "Eu pensei 'mas que dinheiro é esse?' e fui checar", diz.

Ao identificar uma TED, Regina acionou seu banco. "Pedi para devolver, mas disseram que era eu quem tinha de cuidar disso." Ela então ligou para instituição financeira que fez o depósito, disse que não reconhecia aquele crédito, mas foi informada que haviam recebido um contrato assinado por ela.

Nas semanas seguintes, não obteve qualquer explicação. "Se existia um contrato, eu tinha que estar conivente com ele. E eu nunca havia falado nem assinado nada com essa instituição." Regina então acionou a ouvidoria e esperou alguma resposta.

Cerca de um ano depois, a empresa ainda insiste que tinha um contrato assinado por ela. Já a ouvidoria disse apenas que o erro foi cometido por um funcionário, desligado da empresa. Por fim, Regina devolveu o valor que havia sido indevidamente creditado em sua conta, mas segue sem saber como conseguiram seus dados pessoais.

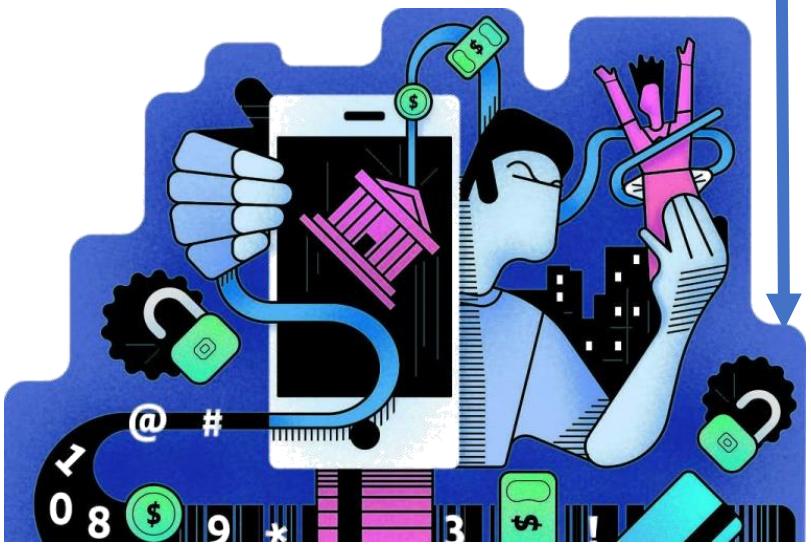
A situação experimentada por Regina enfatiza uma crescente inquietação em relação à privacidade.

De acordo com um estudo conduzido pelo *Massachusetts Institute of Technology* (MIT), houve um expressivo aumento de 493% no número de vazamentos de dados no Brasil entre 2018 e 2019. Em 2018, foram registrados três incidentes significativos, mas esse número saltou para 16 no ano seguinte.

Em janeiro de 2021, ocorreu o vazamento de 223 milhões de registros de dados pessoais de brasileiros, seguido, no mês seguinte, pelo vazamento de 102 milhões de contas de celular. Como resultado desses incidentes, o Brasil agora ocupa a 12ª posição no *ranking* dos países mais afetados por vazamentos de dados.

Disponível em: https://www1.folha.uol.com.br/tec/2022/09/saiba-o-que-fazer-em-caso-de-vazamento-de-dados-pessoais.shtml. Acesso em: 08.09.2023

O que aconteceu com a Sra. Regina, o uso não autorizado de dados para diversos fins e atividades, poderia ter ocorrido com qualquer um de nós. Você já imaginou algum familiar seu nessa mesma situação? Quais ações podem ser tomadas para auxiliar Sra. Regina na resolução desse problema?



# Refletindo sobre...

## Aplicando conhecimentos

1) Duas empresas de segurança cibernética, A e B, apuraram vazamentos de senha em contas de seus usuários nos anos de 2019 e 2020 e identificaram as senhas mais utilizadas conforme tabela a seguir:

| Senhas mais comuns 2019 | | |
|---|---|---|
| Ano / Senhas | Empresa A | Empresa B |
| senha | 830 | 360 |
| 123456 | 2485 | 2543 |
| 123456789 | 10521 | 9614 |
| qwerty | 348 | 156 |

| Senhas mais comuns 2020 | | |
|---|---|---|
| Ano / Senhas | Empresa A | Empresa B |
| senha | 209 | 492 |
| 123456 | 1031 | 1523 |
| 123456789 | 4602 | 4130 |
| qwerty | 227 | 309 |

a) Qual o total de cada senha vazada nas empresas A e B nesses dois anos?

b) Qual a senha com maior número de usuários?

2) Observando a tabela de "Senha mais comuns de 2020", suponha que as empresas A e B resolveram verificar o perfil de seus usuários. Analisando o cadastramento, identificaram que a empresa A tem 50% dos usuários homens e os outros 50% mulheres, já a empresa B revelou ter 80% de seus usuários mulheres e 20% homens, conforme matriz $P=\begin{bmatrix} 0,5 & 0,5 \\ 0,8 & 0,2 \end{bmatrix}$. Qual o número de homens e mulheres que utilizavam cada uma das senhas nas empresas A e B em 2020?

Socializando Informações

3) Você já ouviu falar sobre alguma lei referente à proteção ou segurança de dados? Existe sim, uma lei que garante esta proteção é a Lei Geral de Proteção de Dados (LGPD). Vamos conhecer a LGPD e suas implicações para a proteção de dados pessoais no Brasil? Que tal fazer uma pesquisa e trazer um texto explicativo, no formato de História em Quadrinhos, sobre esta lei e seus benefícios para o cidadão?

Dicas para produção da HQ:

1. Inicie planejando a criação das suas histórias em quadrinhos.
2. Determine o tamanho desejado para sua história.
3. Planeje a distribuição dos quadros de forma estratégica.
4. Explore ao máximo a liberdade criativa que está em suas mãos.
5. Dê atenção especial ao texto dos balões de fala.
6. Familiarize-se com os diferentes tipos de balões que você pode utilizar.
7. Reconheça a importância das onomatopeias na narrativa visual.
8. Procure por *templates* específicos para a criação de histórias em quadrinhos.
9. Inicie os quadros com diálogos e pensamentos dos personagens.
10. Considere um processo inverso na criação de suas histórias em quadrinhos.

Fonte: https://le.com.br/blog/criar-historias-em-quadrinhos/

# Iniciando o Diálogo...

## Problematizando

**Texto IV**

## Continuando a conversa...

A Informática teve um profundo impacto em nossa identidade e comportamento, influenciando decisões cotidianas e tornando-se essencial em todos os aspectos da vida moderna, desde compromissos importantes até atividades de lazer, como dirigir um carro ou fazer compras online. Quem nunca se atrasou para um compromisso importante porque esqueceu seu *smartphone* em casa e sentiu-se desconfortável sem ele? Sua presença é notória e suas transformações são consideradas irreversíveis.


Na era digital, a comunicação e as operações são predominantemente conduzidas por computadores conectados à internet, promovendo conveniência, produtividade e interconexão em tempo real. A Informática e a Matemática estão intimamente ligadas, pois muitos conceitos matemáticos são fundamentais para a Informática, e os matemáticos foram pioneiros na criação dos primeiros computadores, impulsionando a Tecnologia da Informação.

A proteção de informações é crucial para a segurança em interações digitais. Medidas de segurança, como a Criptografia, desempenham um papel essencial nesse sentido, senda a Matemática fundamental para sua construção. A Criptografia é amplamente utilizada em aplicativos de mensagens e na proteção de senhas em dispositivos, garantindo a segurança das comunicações.


Fonte: fasciculo-protecao-de-dados-egc.pdf (cert.br)

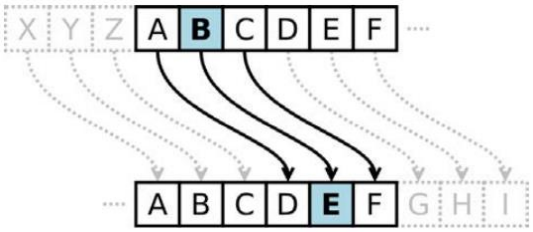
Sempre que uma senha é inserida em um computador, *tablet* ou *smartphone*, ou quando você acessa uma rede social ou Wi-Fi, entra em ação a Criptografia, ou seja, a Matemática desempenha um papel fundamental na garantia da segurança de suas comunicações.

**Atividade III**. Dialogando com o texto

1) Você já parou para pensar na importância da proteção de informações em interações digitais? E sobre o papel da Matemática na garantia da segurança das comunicações digitais? Apresente em algumas linhas suas impressões a partir da leitura do texto.

2) Você já ouviu falar em Criptografia? Como ela contribui para a segurança das comunicações digitais? Em quais situações a Criptografia é amplamente utilizada?

3) A criptografia consiste em codificar e decodificar mensagens para que apenas o emissor e o receptor as conheçam. A primeira criptografia com propósitos militares foi a de Júlio César, conhecida como Cifra de César. Ela é feita substituindo cada letra da mensagem por outra, três casas à frente no alfabeto. Assim, a letra A é trocada por D, B por E, C por F e assim sucessivamente.




Criptografando a palavra "UVA", por exemplo, teríamos "XYD". Para decodificar, basta fazer o processo inverso.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

Agora é sua vez: decifre a mensagem "HX DPR DSUHQGHU PDWHPDWLDF".

4) Observando a Cifra de César, crie uma para codificar a mensagem "ANDAR COM FÉ EU VOU" e escolha um colega de sala para decodificar.

5) Duas amigas, Ana e Bruna, estão trocando mensagens em códigos para que outras pessoas não saibam do que estão conversando. Nesta escrita, elas substituem números por letras conforme a tabela abaixo:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 10 | 22 | 9 | 5 | 4 | 18 | 2 | 17 | 25 | 23 | 12 | 14 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 1 | 19 | 15 | 20 | 21 | 11 | 3 | 16 | 24 | 6 | 13 | 0 |

Ana enviou para Bruna o nome do garoto por quem ela está apaixona, codificado em uma matriz B, de ordem 3x1, e revelou que a chave para decodificar é uma matriz C, de ordem 3x3. Para conhecer a mensagem, Bruna deve multiplicar a matriz C pela matriz B e converter os números em letras usando a tabela acima.

Vejamos as matrizes $B = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}$ e $C = \begin{bmatrix} 1 & 9 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 0 \end{bmatrix}$

Qual é o nome do garoto por quem Ana está apaixonada?

# Organizando o conhecimento

Você já percebeu que as matrizes podem nos auxiliar na codificação e decodificação de mensagens? Utilizando a multiplicação de matrizes, podemos codificar e decodificar mensagens. Para isso, cria-se uma numeração das letras do alfabeto, conforme a tabela abaixo. (O símbolo * corresponde a um espaço).

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | * |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |

Suponha que se deseje enviar a mensagem **FUVEST**, e que a matriz codificadora é $C = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$ e decodificadora seja $D = \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix}$. A matriz da mensagem é $M = \begin{bmatrix} F & U & V \\ E & S & T \end{bmatrix}$, que em números é $M = \begin{bmatrix} 6 & 21 & 22 \\ 5 & 19 & 20 \end{bmatrix}$.

Fazemos o produto das matrizes C.M para codificar a mensagem. Assim, o receptor recebe R:

$$R = C.M = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 6 & 21 & 22 \\ 5 & 19 & 20 \end{bmatrix} = \begin{bmatrix} 3.6 + 2.5 & 3.21 + 2.19 & 3.22 + 2.20 \\ 1.6 + 1.5 & 1.21 + 1.19 & 1.22 + 1.20 \end{bmatrix} = \begin{bmatrix} 28 & 101 & 106 \\ 11 & 40 & 42 \end{bmatrix}$$

O receptor decodifica a mensagem R fazendo o produto D.R e encontra a mensagem M:

$$M = D.R = \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 28 & 101 & 106 \\ 11 & 40 & 42 \end{bmatrix} = \begin{bmatrix} 1.28 + (-2).11 & 1.101 + (-2).40 & 1.106 + (-2).42 \\ -1.28 + 3.11 & -1.101 + 3.40 & -1.106 + 3.42 \end{bmatrix} = \begin{bmatrix} 6 & 21 & 22 \\ 5 & 19 & 20 \end{bmatrix}$$

Para codificar a mensagem, realizamos um procedimento, e para decodificar fazemos o inverso, e isso ocorre com as matrizes. Duas matrizes quadradas de ordem $n$ são inversas quando o produto delas, em qualquer ordem, é igual à matriz identidade de ordem $n$. Indicamos a inversa de uma matriz A por $A^{-1}$. Possuindo inversa, a matriz é chamada de invertível ou inversível.

A matriz decodificadora D é a inversa da matriz codificadora C, isto é, $D = C^{-1}$. O produto entre elas é igual à matriz identidade, vejamos:

$$C.D = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = \begin{bmatrix} 3.1 + 2.(-1) & 3.(-2) + 2.(3) \\ 1.1 + 1.(-1) & 1.(-2) + 1.(3) \end{bmatrix} = \begin{bmatrix} 3 - 2 & -6 + 6 \\ 1 - 1 & -2 + 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

De forma análoga, o produto D.C resulta na matriz identidade de ordem 2.

Suponha que a matriz codificadora da mensagem codificada $N = \begin{bmatrix} 20 & 31 & 4 \\ 35 & 43 & 5 \end{bmatrix}$ recebida pelo receptor é $K = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$. Qual é a matriz decodificadora?

Para conhecer a mensagem, deve-se fazer o produto da matriz decodificadora com a matriz da mensagem recebida. Como a matriz decodificadora $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ é a inversa da matriz codificadora K, precisamos encontrá-la, pois, $A = K^{-1}$.

$K.A = K.K^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a + c & b + d \\ a + 2c & b + 2d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Resolvendo o sistema temos,

$$\begin{cases} a + c = 1 \\ a + 2c = 0 \end{cases} \rightarrow a = 2 \; e \; c = -1 \quad \text{e} \quad \begin{cases} b + d = 0 \\ b + 2d = 1 \end{cases} \rightarrow b = -1 \; e \; d = 1. \text{ Logo, } K^{-1} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix}$$

# Ampliando repertório...

## Aprofundando a leitura

**Texto V**

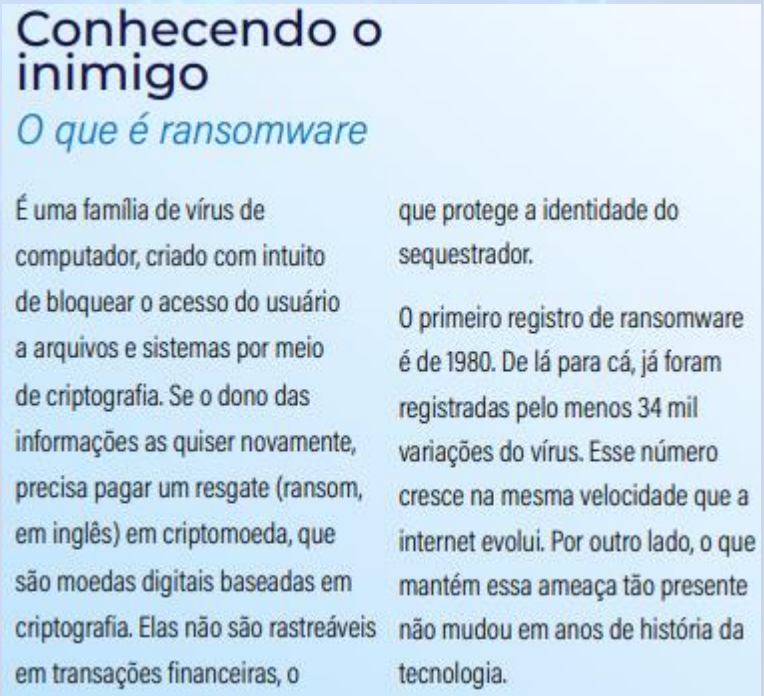
### Afinal, o que é Criptografia?

A palavra tem origem grega e significa *"kripto"* (escondido) e *"grafo"* (grafia). Criptografia, portanto, significa escrita oculta ou secreta. Para cifrar e decifrar uma mensagem, utilizamos um código chamado de **chave**. A primeira e mais simples técnica de criptografar é chamada de Cifra de César. Com o intuito de esconder estratégias e segredos das forças inimigas, generais, reis e rainhas, há milênios, procuravam formas eficientes de comunicação com seus exércitos em guerras, motivando o desenvolvimento de códigos e técnicas para mascarar mensagens, permitindo apenas ao destinatário a leitura de seu conteúdo.

Atualmente, a criptografia é adotada como uma medida de segurança e sua utilização em situações do cotidiano cresceu consideravelmente após o aumento de casos de vazamento de dados. Ela permite ao emissor e receptor entender as mensagens que têm seu teor embaralhado por meio de algoritmos matemáticos. Existem duas categorias ou tipos de criptografia: a simétrica, ou de chave secreta, onde a mesma chave é utilizada para criptografar e descriptografar a mensagem; e a assimétrica, ou de chave pública, em que é utilizado um par de chaves, uma pública para criptografar e outra privada para descriptografar a mensagem.

A criptografia é amplamente utilizada no comércio eletrônico (pagamentos, transações bancárias), no armazenamento de dados, nas comunicações (assinatura digitais, correio eletrônicos, redes Wi-Fi, envio de documentos), na proteção de dados de navegação, no preenchimento de formulários, em sites do governo e na utilização de senhas de acesso.

A criptografia RSA, criada em 1977 por Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman, foi elaborada com um sistema de duas chaves baseadas em teoremas clássicos da Teoria dos Números. Dessa forma, não é possível obter a chave secreta mesmo tendo conhecimento da chave pública. Um exemplo disso são os nossos dados bancários: todos têm acesso ao número da conta, mas a senha apenas o dono da conta conhece, sendo esta informação de acesso privado.



Conhecendo o inimigo

*O que é ransomware*

É uma família de vírus de computador, criado com intuito de bloquear o acesso do usuário a arquivos e sistemas por meio de criptografia. Se o dono das informações as quiser novamente, precisa pagar um resgate (ransom, em inglês) em criptomoeda, que são moedas digitais baseadas em criptografia. Elas não são rastreáveis em transações financeiras, o que protege a identidade do sequestrador.

O primeiro registro de ransomware é de 1980. De lá para cá, já foram registradas pelo menos 34 mil variações do vírus. Esse número cresce na mesma velocidade que a internet evolui. Por outro lado, o que mantém essa ameaça tão presente não mudou em anos de história da tecnologia.

https://ish.com.br/wp-content/uploads/2021/09/ISH-ebook-Ransomware-Entendendo_o_inimigo.pdf

# Vamos decifrar mais uma mensagem?

Utilizando a transposição de letras para codificar e decodificar mensagens e o conceito de matriz transposta, vamos decifrar a mensagem a seguir:

***SICNAERHÃSCDÃOSAOOPA***

Na escrita codificada da mensagem, não levamos em consideração espaços ou sinais de pontuação. A noção de números primos e compostos nos auxiliará a formar a matriz codificada. Sigamos o passo a passo:

Primeiro, contamos o número de letras na mensagem. No passo seguinte, escrevemos essa quantidade como um produto de dois números. Por exemplo, na mensagem "***Nem tudo que reluz é ouro***", temos 20 letras. Podemos escrever 20 como 1x20; 2x10; 4x5; 5x4; 10x2; e 20x1.

Vamos utilizar esses produtos para compor a matriz onde será decodificada a mensagem. Demarcando que o primeiro número do produto vai representar o número de linhas e o segundo, o número de colunas, escreveremos a matriz $M(a_{ij})_{mxn}$.

Descartando os produtos 1x20 (matriz linha) e 20x1(matriz coluna), pois são matrizes que não permitem embaralhar as letras, logo não é possível realizar a encriptação. Optaremos pelo produto 4x5, inserindo a mensagem em uma tabela de 4 linhas e 5 colunas. Em seguida, substituímos as letras pelos números correspondentes, conforme tabelas a seguir:

| | | | | |
|---|---|---|---|---|
| N | E | M | T | U |
| D | O | Q | U | E |
| R | E | L | U | Z |
| É | O | U | R | O |

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | * |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |

A matriz associada a tabela é $M=\begin{bmatrix} 14 & 5 & 13 & 20 & 21 \\ 4 & 15 & 17 & 21 & 5 \\ 18 & 5 & 12 & 21 & 26 \\ 5 & 15 & 21 & 18 & 15 \end{bmatrix}_{4x5}$. Escrevemos a mensagem em linhas.

Para criptografar, vamos escrever as linhas da matriz M ordenadamente na posição de colunas. Assim, teremos $R=\begin{bmatrix} 14 & 4 & 18 & 5 \\ 5 & 15 & 5 & 15 \\ 13 & 17 & 12 & 21 \\ 20 & 21 & 21 & 18 \\ 21 & 5 & 26 & 15 \end{bmatrix}_{5x4}$

A mensagem criptografada é "**NDREEOEOMQLUTUURUEZO**". Para decodificar a mensagem, basta fazer o processo inverso.

Na situação acima, a chave para codificar mensagem foi reorganizar a matriz escrevendo os elementos que compõe a linha no lugar da coluna. Este procedimento é representado por uma matriz conhecida como **Matriz Transposta**. Indicamos a transposta da matriz M por $M^t$, em que $M^t$ é obtida trocando-se, ordenadamente, as linhas pelas colunas de M. Ou seja, se a ordem de M é ***mxn*** a ordem de $M^t$ será ***nxm***.

# Refletindo sobre...

## Aplicando conhecimentos

1) No Texto V apresentado na seção “Aprofundando a leitura”, vimos um pouco mais sobre a criptografia e outros conceitos relacionados, como *ransomware* e criptomoeda. O primeiro existe desde a década de 1980, enquanto as criptomoedas são mais recentes. Você sabe o que é uma criptomoeda? Quando surgiu e quem a inventou? Apresente exemplos de situações que as envolvem.

2) Vamos decifrar a mensagem apresentada no início do texto? Você terá 10 minutos para decodificá-la.

***SICNAERHÃSCDÃOSAOOPA***

3) Retomando a mensagem codificada $N=\begin{bmatrix}20 & 31 & 4\\35 & 43 & 5\end{bmatrix}$ recebida pelo receptor, na página 22, vimos que a matriz codificadora $K=\begin{bmatrix}1 & 1\\1 & 2\end{bmatrix}$ foi fornecida e encontramos a chave para descriptografar a mensagem, a matriz inversa $K^{-1}$. De acordo com essas informações, qual foi a mensagem enviada?

Socializando Informações

No período da Segunda Guerra Mundial, a criptografia entrou na era mecânica com o surgimento da máquina Enigma. A quebra do código da máquina Enigma marcou a criptoanálise e foi realizada por Alan Turing e seus colaboradores. O filme “O jogo da Imitação” conta essa história. Vamos conferir?

Assista ao filme, escolha sua melhor cena e crie um *padlet* com um pequeno resumo sobre ela.


Dicas para produção do *padlet*:

1. Escolha um design visualmente atraente.
2. Dê um título claro e uma descrição breve
3. Escolha o layout apropriado.
4. Utilize textos, imagens, vídeos, links e arquivos.
5. Organize o conteúdo de forma lógica.
6. Divida o conteúdo em seções ou categorias.
7. Permita colaboração e feedback.
8. Escolha fontes e cores legíveis.
9. Defina configurações de privacidade apropriadas.
10. Compartilhe o link do *padlet* de maneira eficaz.

# Pesquisa e Investigação

Que tal aprofundar um pouco mais no universo da Criptografia? A proposta é que seja feito um seminário sobre “A importância da Criptografia na Segurança Digital”. O seminário permitirá que façamos um passeio por vários subtemas ligados à Criptografia. A proposta é que seja realizada uma pesquisa em grupo e que os resultados sejam compartilhados no seminário. Cada grupo de estudantes escolherá um tópico para se aprofundar, vejamos algumas sugestões:

- Cifra de Hill;
- Cifra de Playfair;
- Cifra de Vigenère;
- Cifra de Fustel;
- Código enigma;
- Criptografia simetria e assimétrica;
- Segurança de rede;
- Assinatura digital;
- Criptografia ASCII;
- Criptografia Quântica;
- Criptografia RSA.

# Referências


ANDRADE, E. **A História da Criptografia.** Disponível em: <http://www.dsc.ufcg.edu.br/~pet/jornal/abril2014/materias/historia_da_computacao.html>. Acesso em: 19 fev. 2024.

CONVERGÊNCIA DIGITAL. Trinta milhões de senhas foram vazadas no Brasil em 2022. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Trinta-milhoes-de-senhas-foram-vazadas-no-Brasil-em-2022-63146.html?UserActiveTemplate=mobile. Acesso em: 13 jun. 2024.

DE, A. et al. **Uma Sequência Didática para o Ensino**. [s.l: s.n.]. Disponível em: <https://educapes.capes.gov.br/bitstream/capes/644426/1/Antonino%20de%20Ara%C3%BAjo%20Farias%20PRODUTO%20EDUCACIONA.pdf>. Acesso em: 19 fev. 2024.

KRANZ, B., OLGIN, C., Construção de conhecimentos matemáticos utilizando a temática criptografia para o Ensino Médio. **Revista de Ensino de Ciências e Matemática** [en linea]. 2021, 12(3), 1-21[fecha de Consulta 18 de Febrero de 2024]. ISSN: . Disponible en: http://portal.amelica.org/ameli/journal/509/5092220025/

LE.COM.BR. **Criar Histórias em Quadrinhos**. Disponível em: https://le.com.br/blog/criar-historias-em-quadrinhos/.

MALAGUTTI, Pedro Luiz; BEZERRA, Débora de Jesus; RODRIGUES, Vânia Cristina da Silva. Aprendendo criptologia de forma divertida. 2010.

MEDICO, Lucilene Dal. O ensino-aprendizagem de matrizes e determinantes por meio de resolução de problemas. 2008. 141 f. Dissertação (Mestrado em Ensino de Matemática) - Universidade Franciscana, Santa Maria, 2008.

NordPass. **200 contraseñas más comunes del 2022**. Disponível em: https://s1.nordcdn.com/nord/misc/0.78.0/nordpass/top-200-2023/200-most-common-passwords-es.pdf.

OLIVEIRA, Reinaldo Donizete de. Utilização de mensagens criptografadas no ensino de matrizes. 2013.

SAFERNET BRASIL. **Segurança Digital**. Disponível em: https://new.safernet.org.br/content/seguran%C3%A7a-digital. Acesso em: 19 fev. 2024.

SAFERNET BRASIL**. Indicadores Helpline**. Disponível em: <https://indicadores.safernet.org.br/helpline/helplineviz/helpchart-page.html>. Acesso em: 19 fev. 2024.

SANJUAN, Gemma Calbo; LÓPEZ, Juan Carlos Cortés. Aplicación de las matrices invertibles en criptografía. **Ensayos: Revista de la Facultad de Educación de Albacete**, n. 18, p. 279, 2003.

UNIVESP. **Univesp | Matrizes e Criptografia**. Disponível em: <https://apps.univesp.br/matrizes-e-criptografia/>. Acesso em: 19 fev. 2024.