

# Segurança da Informação

**Diretrizes para atualização e proteção dos  
equipamentos de TI**

**Fábio Nogueira da Silva**

Equipe da Seção de Proteção de Dados e Segurança da Informação

SETIC



# Conteúdo

1. O que é a Informação
2. Proteção da informação e a importância dos colaboradores nesse processo
3. Principais ataques à segurança da informação
  - Engenharia social
4. Semana da Segurança da Informação – segunda etapa
  - O que fazer para não ter a Internet interrompida no dia 29/11.



# O que é a informação?

- O ativo estratégico mais importante de uma organização.
- É um conjunto de conhecimento organizado pertencente a determinada organização, podendo ser de domínio público ou privado.

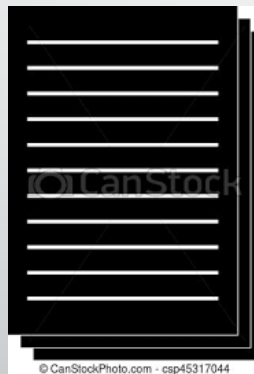
# Distribuição da informação



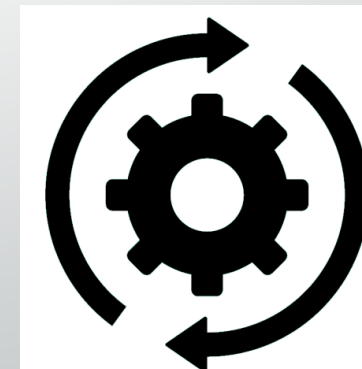
Pessoas



Equipamentos de TI



Papéis e documentos



Sistemas e processos de trabalho

# Precisamos proteger a informação



# Desafios para proteção da informação



Níveis de Segurança, Risco e Flexibilidade

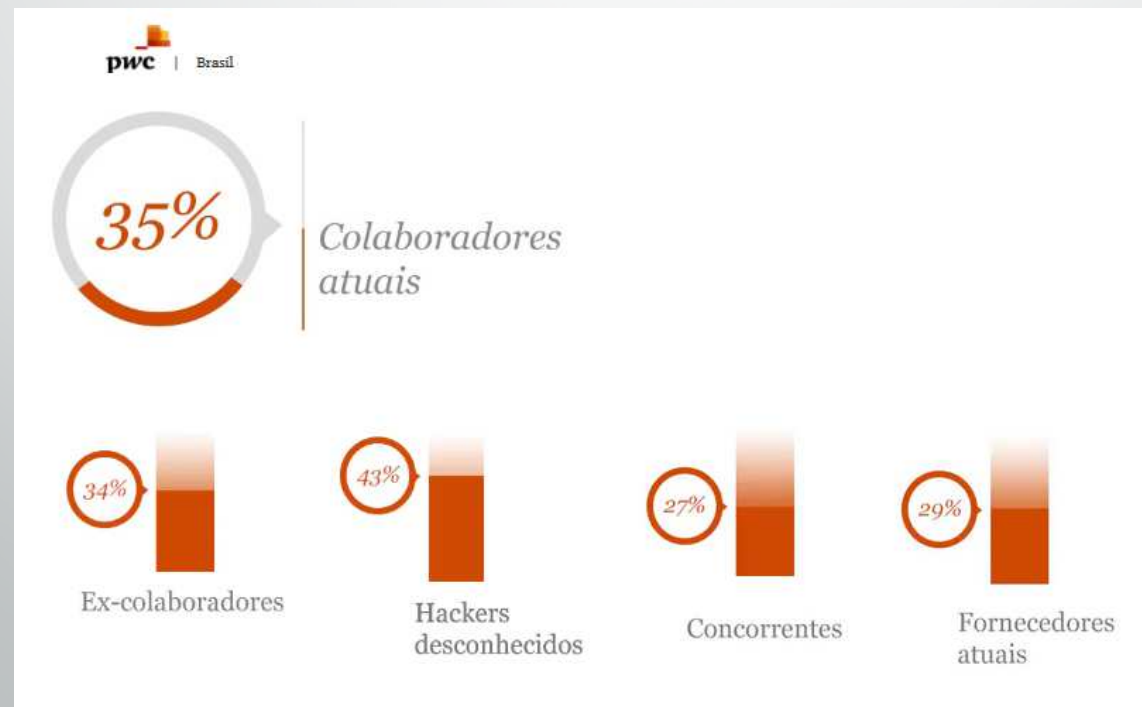


Precisamos  
de  
você



# Por que você é tão importante ?

- Pesquisa mundial da PWC 2018 [1] - mostra que as violações de segurança ocorrem, em sua grande maioria, **INTERNAMENTE** (Colaboradores e ex-colaboradores).





# Por que você é tão importante ?

- Pesquisa da empresa Eset (2019/2020) mostra aumento de 200% no número de ataques de engenharia social no Brasil.



# Por que você é tão importante ?

- Somo o segundo país da América Latina em quantidade de ataques desse tipo (engenharia social).



# Por que você é tão importante ?

- Engenharia social: conjunto de ataques realizados por cibercriminosos que tem como objetivo enganar as pessoas para violação da segurança da informação.
- Atualizações de segurança, ferramentas de última geração e outras medidas NÃO são tão BOAS quanto COLABORADORES treinados e aptos a identificarem esse tipo de armadilha.

# Por que você é tão importante ?

- Diversos ataques recentes a órgãos públicos com o crescimento do trabalho remoto:
  - TJ/RS – ransoware
  - TRT<sub>4</sub> - ransoware
  - TJ/SP - ransoware
  - STJ - ransoware
  - STF – Sql Injection

# Por que você é tão importante ?

- Notícias recentes de ataques cibernéticos

06/05/2021

**G1** RIO GRANDE DO SUL 

## Nove dias após ataque cibernético, TJ-RS ainda enfrenta dificuldades para acessar processos

Cerca de 75% dos arquivos do Tribunal de Justiça gaúcho estão inacessíveis. Polícia ainda não identificou responsáveis pelo ataque.

Por Léo Saballa Jr., RBS TV  
06/05/2021 21h15 - Atualizado há uma semana

[f](#) [t](#) [w](#) [i](#) [p](#)

07/05/2021

**G1** POLÍTICA

## Supremo investiga suposto ataque hacker a sistema da Corte

Site do STF foi tirado do ar e, segundo a Corte, retomada é gradual. Nota diz que só foram acessados dados públicos e que ataque não atrapalhou atuação do Supremo.

Por Márcio Falcão e Fernanda Vivas, TV Globo — Brasília  
07/05/2021 10h55 - Atualizado há uma semana

[f](#) [t](#) [w](#) [i](#) [p](#)

04/11/2020

**G1** POLÍTICA

## STJ diz que sistema de informática do tribunal foi alvo de ataque hacker e pede investigação da PF

Técnicos verificaram indisponibilidade do sistema nesta terça (3). Eles afirmaram ter encontrado arquivo que pode ser vírus. Presidente do STJ decidiu suspender sessões temporariamente.

Por Márcio Falcão e Fernanda Vivas, TV Globo — Brasília  
04/11/2020 10h52 - Atualizado há 6 meses

[f](#) [t](#) [w](#) [i](#) [p](#)

12/05/2017

**G1** SÃO PAULO

## Ciberataque faz sistema do Tribunal de Justiça de SP cair; sites do MP e do TRT também saem do ar

Judiciário paulista admitiu que computadores foram infectados, o que motivou o desligamento de todas as máquinas da instituição. INSS informa que suspendeu atendimentos nesta sexta.

Por G1 São Paulo  
12/05/2017 13h45 - Atualizado há 4 anos

[f](#) [t](#) [w](#) [i](#) [p](#)

# Por que você é tão importante ?

- Notícias recentes de ataques cibernéticos

01/12/2020

**G1** VALE DO PARAÍBA E REGIÃO VAN LOAR DA

## Embraer é alvo de ataque cibernético e investiga impactos

Fabricante de aeronaves brasileira informou que realiza procedimentos de investigação para apurar a origem e consequências do ataque hacker.

Por G1 Vale do Paraíba e Região  
01/12/2020 07h42 · Atualizado há 5 meses

f t w l i n p

10/05/2021

**G1** ECONOMIA  
TECNOLOGIA

## O ataque de hackers a maior oleoduto dos EUA que fez governo declarar estado de emergência

Um grupo de hackers desconectou completamente um oleoduto e roubou mais de 100 GB de informações.

Por BBC  
10/05/2021 10h51 · Atualizado há uma semana

f t w l i n p

24/02/2021

**G1** ECONOMIA  
TECNOLOGIA

## Ataques hacker a hospitais e farmacêuticas aumentam com a pandemia, aponta IBM

Organizações e empresas ligadas ao combate à Covid-19 foram duas vezes mais atacadas pelos cibercriminosos em 2020 na comparação com o ano anterior.

Por G1  
24/02/2021 17h46 · Atualizado há 2 meses

f t w l i n p

19/05/2021

Menu NEWS CONTIENDO O MUNDO

## Hackers alteravam processos federais para sacar indenização em Campo Grande

Eles invadiam as ações do TRF3 para obter vantagens financeiras e viraram alvo de Operação da PF nesta quarta

Por Gupy Games | 19/05/2021 14:17

f t w l i n p



# Por que você é tão importante ?

- Notícias recentes de ataques cibernéticos

30/09/2021

The screenshot shows the website of the 4th Regional Labor Court (TRT-4). The header includes the logo for 180 years of the court, the text 'JUSTIÇA DO TRABALHO TRT da 4ª Região (RS)', and a 'CIBERARAR 2º GRAU' badge. On the right, there are social media icons and a search bar labeled 'Pesquisar'. The navigation menu contains: Institucional | Serviços | Notícias | Jurisprudência | Transparência | Legislação | Ouvidoria | Contato. The article is dated 01/10/2021 19:31 and is titled 'COMUNICADO: Ataque cibernético na infraestrutura tecnológica do TRT-RS'. The text of the article states that the administration of the TRT-4 is publicly communicating that on 30.09.2021, around 12:00, suspicious records of malicious activities were detected in the IT infrastructure. It further states that immediately after the attack, the technical team of the SETIC (Secretaria de Tecnologia da Informação e Comunicações do TRT4) executed isolation and containment measures to preserve security and integrity.

**180** anos JUSTIÇA DO TRABALHO TRT da 4ª Região (RS) CIBERARAR 2º GRAU

Sou 100% PJe Pesquisar

Institucional | Serviços | Notícias | Jurisprudência | Transparência | Legislação | Ouvidoria | Contato

01/10/2021 19:31

## COMUNICADO: Ataque cibernético na infraestrutura tecnológica do TRT-RS

A Administração do Tribunal Regional do Trabalho da 4ª Região – TRT4 vem a público comunicar que, no dia 30.09.2021 (quinta-feira), por volta das 12 horas, foram detectados registros suspeitos de atividades maliciosas na infraestrutura tecnológica do TRT4.

Imediatamente após a confirmação do ataque cibernético, a equipe técnica da Secretaria de Tecnologia da Informação e Comunicações do TRT4 (SETIC) executou as medidas de isolamento e contenção dos danos potenciais, a fim de preservar a segurança e a integridade das informações.

# Principais ataques à Segurança da Informação e contramedidas

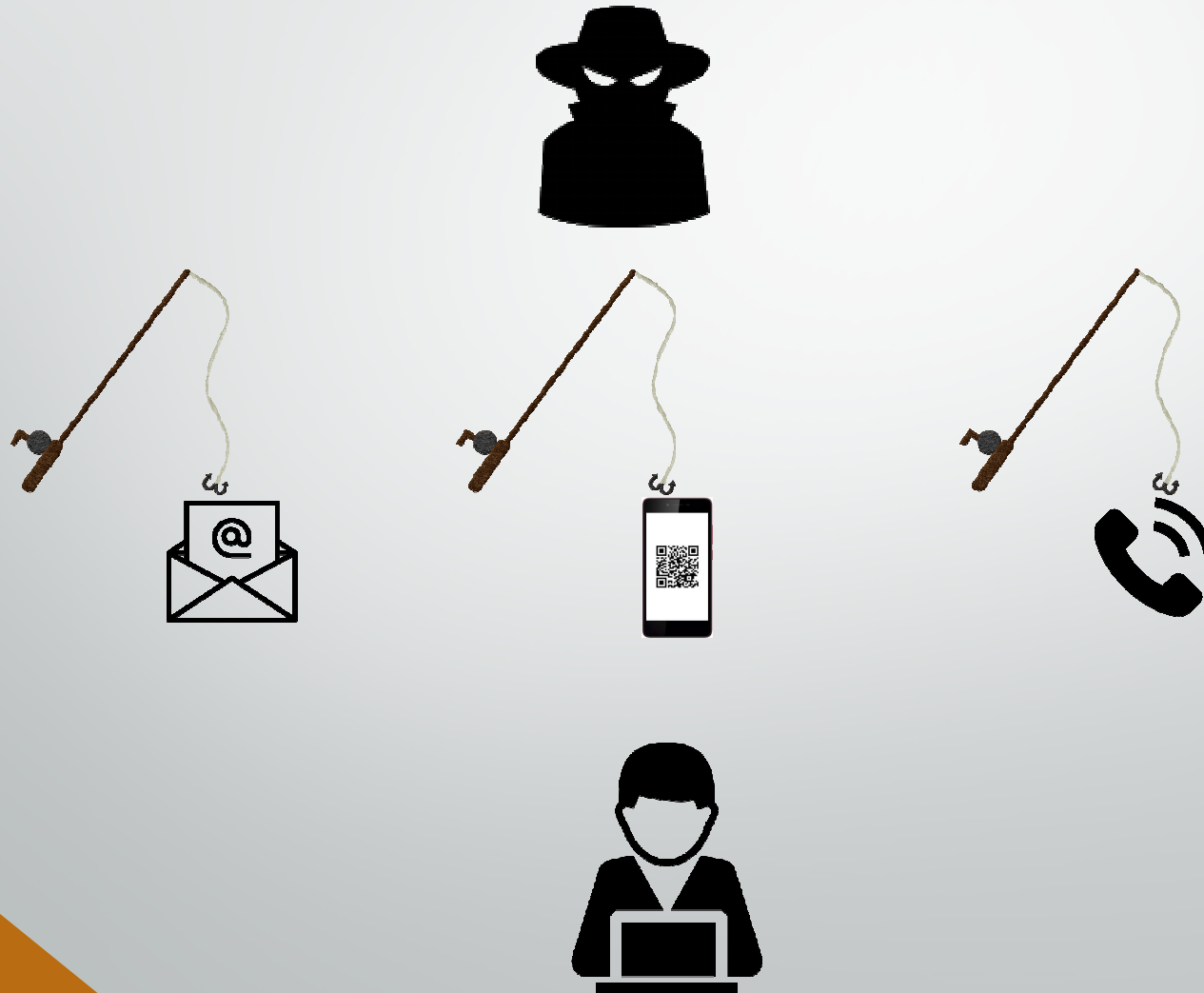


# Principais ataques à Segurança da Informação e contramedidas

- Engenharia social
  1. Phishing;
  2. XSS, injeções e "DNS Poisoning";
  3. Ransoware;
  4. Quebra de senhas;

- Engenharia social

1. Phishing: enganar as pessoas por qualquer meio para compartilhamento de informações pessoais ou execução de ações indesejadas.



- Engenharia social

1. Phishing: Tentativa de induzir o usuário a clicar em uma URL **parecida** com a verdadeira.

De: MercadoLivre <nao-responda@mercadolivre-venda.com>

Data: 13 de abril de 2017 22:53:12 AMT

Para: <izabelamarini@hotmail.com>

Assunto: Enc.: Você vendeu Iphone 7 128gb

Responder A: <nao-responda@mercadolivre-venda.com>



mercado  
livre



Bom trabalho! Você vendeu!



Anúncio #858036391

Iphone 7 Dourado - 128 Gb

Quantidade: 1

R\$ 3,200,00 unid.



### Pagamento

O Seu comprador (a) escolheu a forma de pagamento por cartão

MercadoLivre, o cartão

MercadoLivre é uma parceria entre o MercadoLivre e a rede Visa, O

serviço permite que os compradores efetuem o pagamento de forma

<https://myaccount.mercadolivre.com.br/sales/vop?orderId=1206193693>

- Engenharia social
  1. Phishing: Tentativa de induzir o usuário a clicar em uma URL **parecida** com a verdadeira.

De: MercadoLivre <[nao-responda@mercadolivre-venda.com](mailto:nao-responda@mercadolivre-venda.com)>  
Data: 13 de abril de 2017 22:53:12 AMT  
Para: <[izabelamarini@hotmail.com](mailto:izabelamarini@hotmail.com)>  
Assunto: Enc.: Você vendeu Iphone 7 128gb  
Responder A: <[nao-responda@mercadolivre-venda.com](mailto:nao-responda@mercadolivre-venda.com)>



https://registro.br/tecnologia/ferramentas/whois/?search=mercadolivre-venda.com. Pesquisar

# Whois

Consulta inválida Exibir resultado completo





- Engenharia social

1. Phishing: Tentativa de induzir o usuário a clicar em uma URL **parecida** com a verdadeira.

De: MercadoLivre <[nao-responda@mercadolivre-venda.com](mailto:nao-responda@mercadolivre-venda.com)>

Data: 13 de abril de 2017 22:53:12 AMT

Para: <[izabelamarini@hotmail.com](mailto:izabelamarini@hotmail.com)>

Assunto: Enc.: Você vendeu Iphone 7 128gb

Responder A: <[nao-responda@mercadolivre-venda.com](mailto:nao-responda@mercadolivre-venda.com)>



https://registro.br/tecnologia/ferramentas/whois/?search=mercadolivre-venda.com.br

Whois

mercadolivre-venda.com.br

Recurso inexistente: mercadolive-venda.com.br

Exibir resultado completo

- Engenharia social
  1. Phishing: Tentativa de induzir o usuário a clicar em uma URL **parecida** com a verdadeira.

**De:** MercadoLivre <[nao-responda@mercadolivre-venda.com](mailto:nao-responda@mercadolivre-venda.com)>  
**Data:** 13 de abril de 2017 22:53:12 AMT  
**Para:** <[izabelamarini@hotmail.com](mailto:izabelamarini@hotmail.com)>  
**Assunto:** Enc.: Você vendeu Iphone 7 128gb  
**Responder A:** <[nao-responda@mercadolivre-venda.com](mailto:nao-responda@mercadolivre-venda.com)>



https://registro.br/tecnologia/ferramentas/whois/?search=mercadolivre.com.br


# Whois

mercadolivre.com.br

Exibir resultado completo

## Domínio mercadolive.com.br

TITULAR	MercadoLivre. com Atividades de Internet Ltda.
DOCUMENTO	<a href="#">03.361.252/0001-34</a>
RESPONSÁVEL	Stelleo Tolda
PAÍS	BR
CONTATO DO TITULAR	DOM46



- Engenharia social
  1. Phishing: Tentativa de induzir o usuário a clicar em uma URL **parecida** com a verdadeira.

De: MercadoLivre <[nao-respondamercadolivre-venda.com](mailto:nao-respondamercadolivre-venda.com)>

Data: 13 de abril de 2017 22:53:12 AMT

Para: <[izabelamarini@hotmail.com](mailto:izabelamarini@hotmail.com)>

Assunto: Enc.: Você vendeu Iphone 7 128gb

Responder A: <[nao-respondamercadolivre-venda.com](mailto:nao-respondamercadolivre-venda.com)>



		REPÚBLICA FEDERATIVA DO BRASIL			
CADASTRO NACIONAL DA PESSOA JURÍDICA					
NÚMERO DE INSCRIÇÃO 03.361.252/0001-34 MATRIZ	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL		DATA DE ABERTURA 18/08/1999		
NOME EMPRESARIAL <b>MERCADOLIVRE.COM ATIVIDADES DE INTERNET LTDA</b>					
TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA) *****					PORTE <b>DEMAIS</b>
CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL <b>74.90-1-04 - Atividades de intermediação e agenciamento de serviços e negócios em geral, exceto imobiliários</b>					
CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS <b>82.20-2-00 - Atividades de teleatendimento</b>					
CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA <b>206-2 - Sociedade Empresária Limitada</b>					
LOGRADOURO <b>AV DAS NAÇÕES UNIDAS 3000</b>			NÚMERO <b>3003</b>	COMPLEMENTO <b>PARTE D</b>	
CEP <b>06.233-903</b>	BAIRRO/DISTRITO <b>BONFIM</b>	MUNICÍPIO <b>OSASCO</b>		UF <b>SP</b>	
ENDEREÇO ELETRÔNICO <b>CONSULTASMLB@MERCADOLIVRE.COM</b>			TELEFONE <b>(11) 2543-4155</b>		

- Engenharia social

1. Phishing: Tentativa de induzir o usuário a clicar em uma URL **parecida** com a verdadeira.

No caso de duvidas entre em **contato** conosco.

Sucesso,  
Equipe do MercadoLivre.



<mailto:mercadolivre@mercadolivre-venda.com>

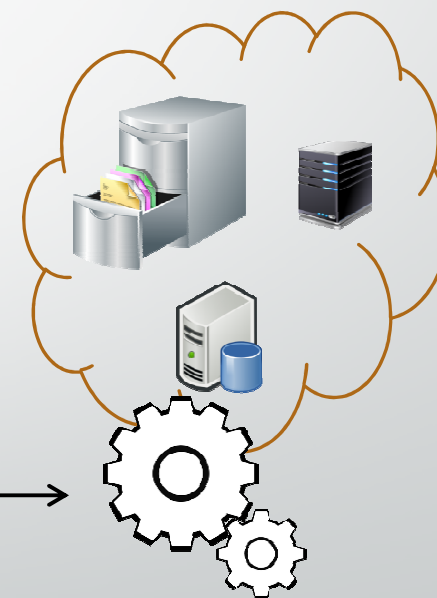
- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso;
    - Como funciona um site ou aplicação Web ?

**Navegador web do seu computador**



**Parte da aplicação Pje rodando no navegador do seu computador**

**Equipamentos TRT24**



**Parte da aplicação Pje rodando nos equipamentos do TRT24**

- Engenharia social
  - 2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso
    - XSS – Cross Site Scripting e pontos de injeção

### Navegador web do computador



Parte da aplicação Pje rodando no navegador do seu computador



- Engenharia social
  2. XSS, injeções e "DNS Poisoning": Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso;
    - XSS – Cross Site Scripting e pontos de injeção

### Navegador web do computador

Advogados - Atualização Cadastral

Nome Completo\*  
Aquilae Oroni

Data de Nascimento\*  
02/04/1909

Brasileiro?  
 Sim  Não

Nome do Pai  
milza

Nome da Mãe\*  
Orionis Sadir

OAB  
Inscrição\* 74232 Letra Seccional\* MT Tipo de Inscrição\* Advogado

CPF\* 621.632.503-50 Sexo\* Masculino

Endereço  
CEP (99999-999) 30140-000 Estado MINAS GERAIS Cidade BELO HORIZONTE Bairro Santa Efigênia  
Logradouro Avenida Brasil Número 356 Complemento  
Telefone\* 31 567890123 E-mail\* aquilae@gmail.com  Incluir processos no Push automaticamente

\* Campos Obrigatórios

Atualizar

Parte da aplicação PJe rodando no navegador do seu computador

- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso
    - XSS – Cross Site Scripting e pontos de injeção;

### Formação da URL de ataque



`https://pje.trt24.jus.br/primeirograu/login.seam?oca%9ks&#093cacao=<script>evil.js</script>..`



Parte da aplicação PJe rodando no navegador do computador

- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso
    - XSS – Cross Site Scripting e pontos de injeção;

## Phishing para finalizar o ataque

**De:** AdministradorPJe <[nao-responda@trt24-jus-br.com](mailto:nao-responda@trt24-jus-br.com)>  
**Data:** 28 de outubro de 2021 13:43:12 AMT  
**Para:** <[fabio.nogueira86@gmail.com](mailto:fabio.nogueira86@gmail.com)>  
**Assunto:** Altere o PIN do seu [token](#) para não perder o acesso ao [PJe](#)



Prezado usuário,

Estamos modificando nosso modelo de autenticação para melhor atendê-lo e trazer mais segurança ao nosso sistema. Pedimos, por gentileza, que altere o número PIN do seu certificado para atendimento à política de alteração de senhas. Segue link para acesso rápido:

<https://pje.trt24.jus.br/primeirograu/login.seam?0ca%9ks&#093acao=<script>evil.js</script>>

Atenciosamente:  
Equipe de TI do TRT24

- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso
    - XSS – Cross Site Scripting e pontos de injeção;

## Phishing para finalizar o ataque

**De:** AdministradorPJe <[nao-responda@trt24-jus-br.com](mailto:nao-responda@trt24-jus-br.com)>

**Data:** 28 de outubro de 2021 13:43:12 AMT

**Para:** <[fabio.nogueira86@gmail.com](mailto:fabio.nogueira86@gmail.com)>

**Assunto:** Altere o PIN do seu token para não perder o acesso ao PJe



Prezado usuário,

Estamos modificando nosso modelo de autenticação para melhor atendê-lo e trazer mais segurança ao nosso sistema. Pedimos, por gentileza, que altere o número PIN do seu certificado para atendimento à política de alteração de senhas. Segue link para acesso rápido:

[Clique aqui para alterar PIN](#)

Atenciosamente:

Equipe de TI do TRT24

- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso
    - XSS – Cross Site Scripting e pontos de injeção;

### Phishing para finalizar o ataque



Prezado usuário,

Estamos modificando nosso modelo de autenticação para melhor atendê-lo e trazer mais segurança ao nosso sistema. Pedimos, por gentileza, que altere o número PIN do seu certificado para atendimento à política de alteração de sen

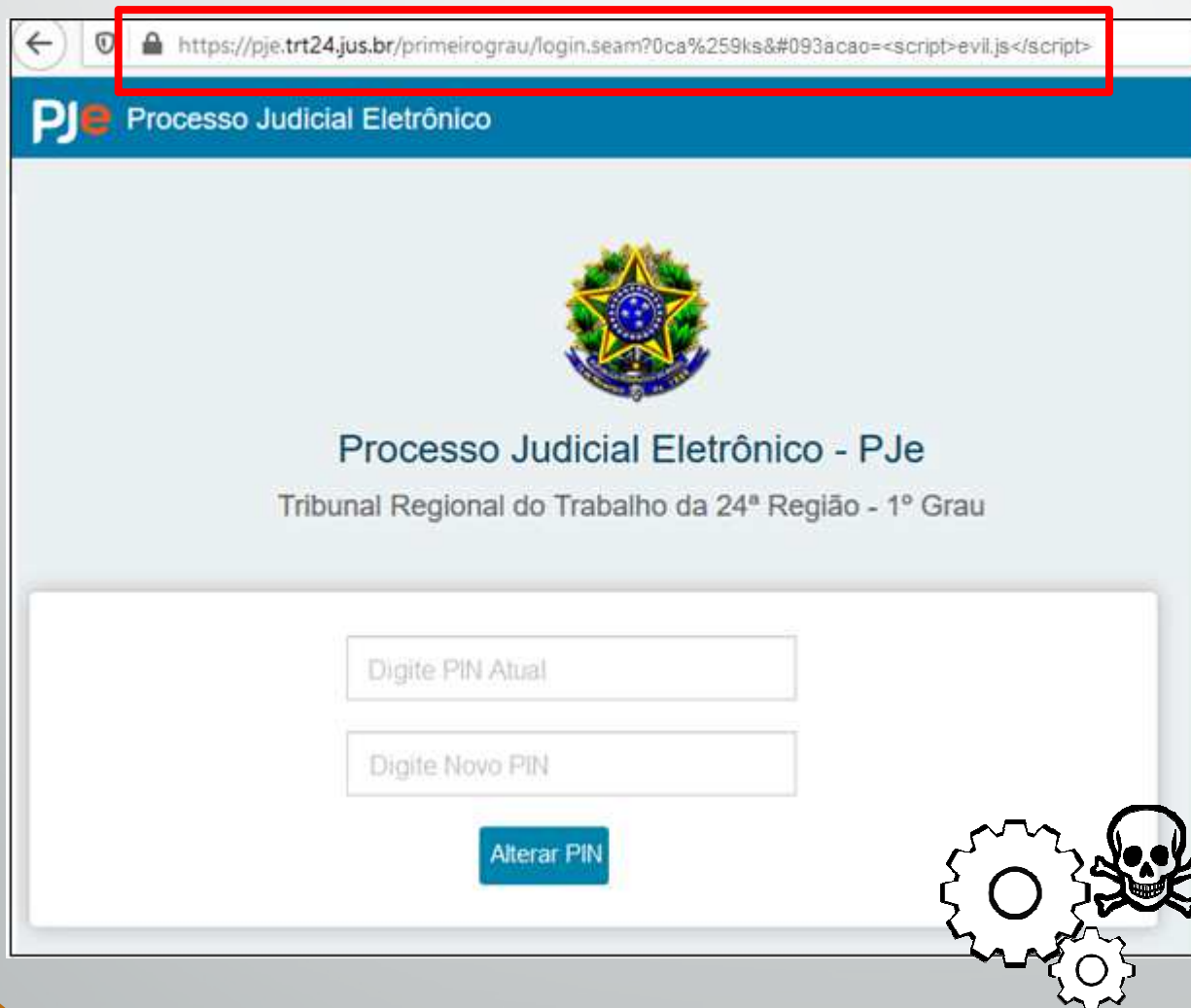
<https://pje.trt24.jus.br/primeirograu/login.seam?0ca%9ks&#093acao=<script>evil.js</script>>

rápido:

Ctrl+clique para seguir o link

[Clique aqui para alterar PIN](#)

- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso
    - XSS – Cross Site Scripting e pontos de injeção;





- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso
    - XSS – Cross Site Scripting e pontos de injeção: como evitar?



- Engenharia social

- 2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso

- XSS – Cross Site Scripting e pontos de injeção: como evitar?

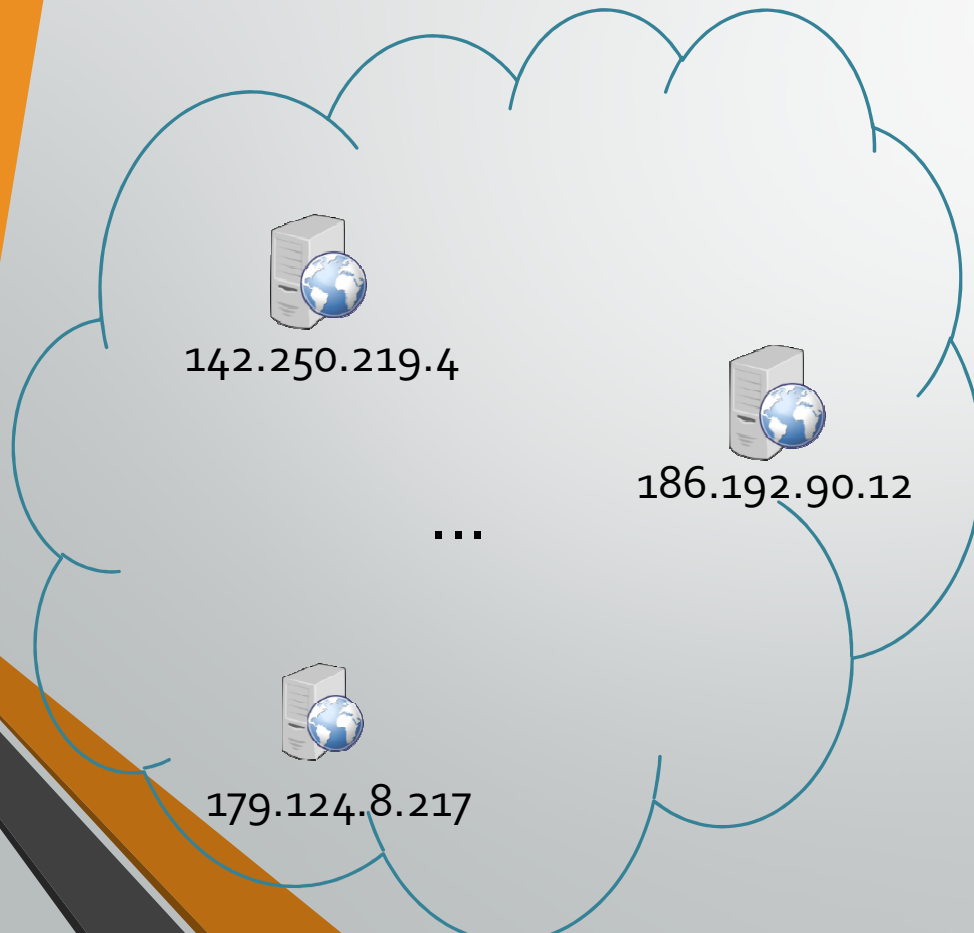


- Engenharia social

- 2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;

- DNS Poisoning – envenenamento de DNS

Servidor DNS



142.250.219.4 -> google.com

179.124.8.217 -> pje.trt24.jus.br

186.192.90.12 -> globo.com

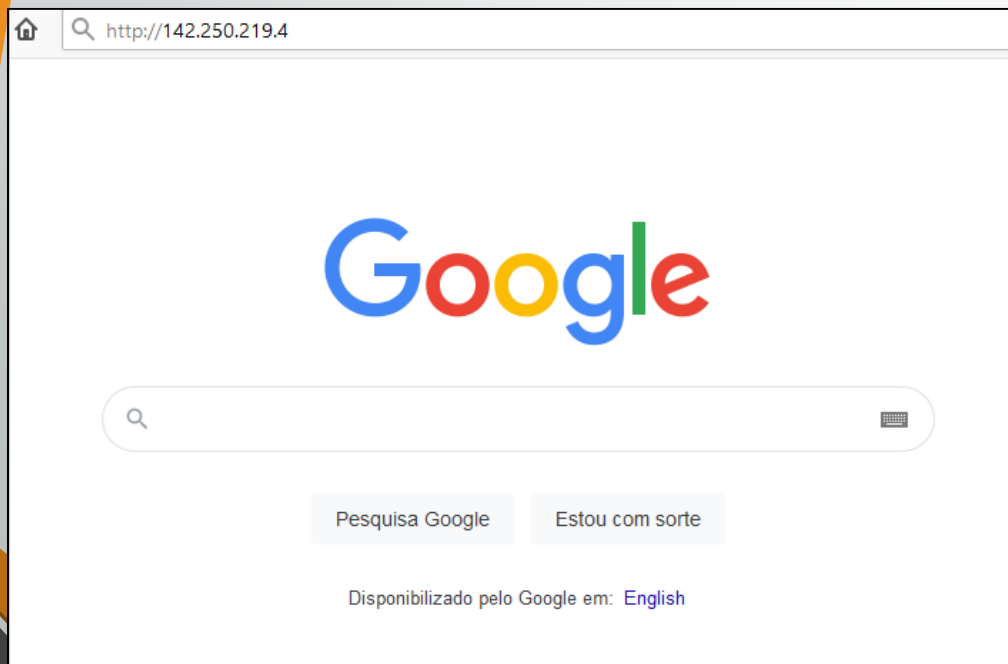
...

- Engenharia social

- 2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;

- DNS Poisoning – envenenamento de DNS

Servidor DNS



142.250.219.4 -> google.com

179.124.8.217 -> pje.trt24.jus.br

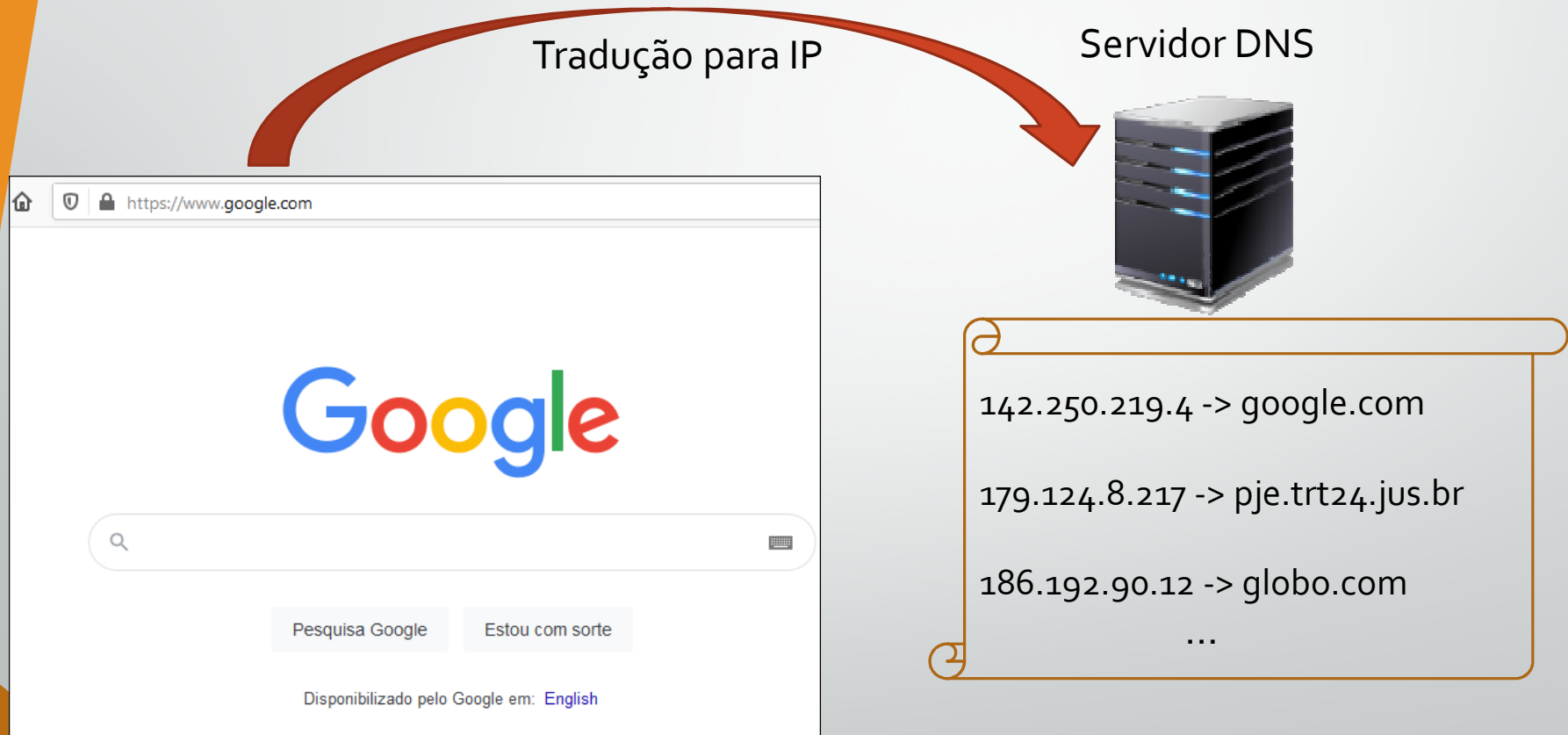
186.192.90.12 -> globo.com

...

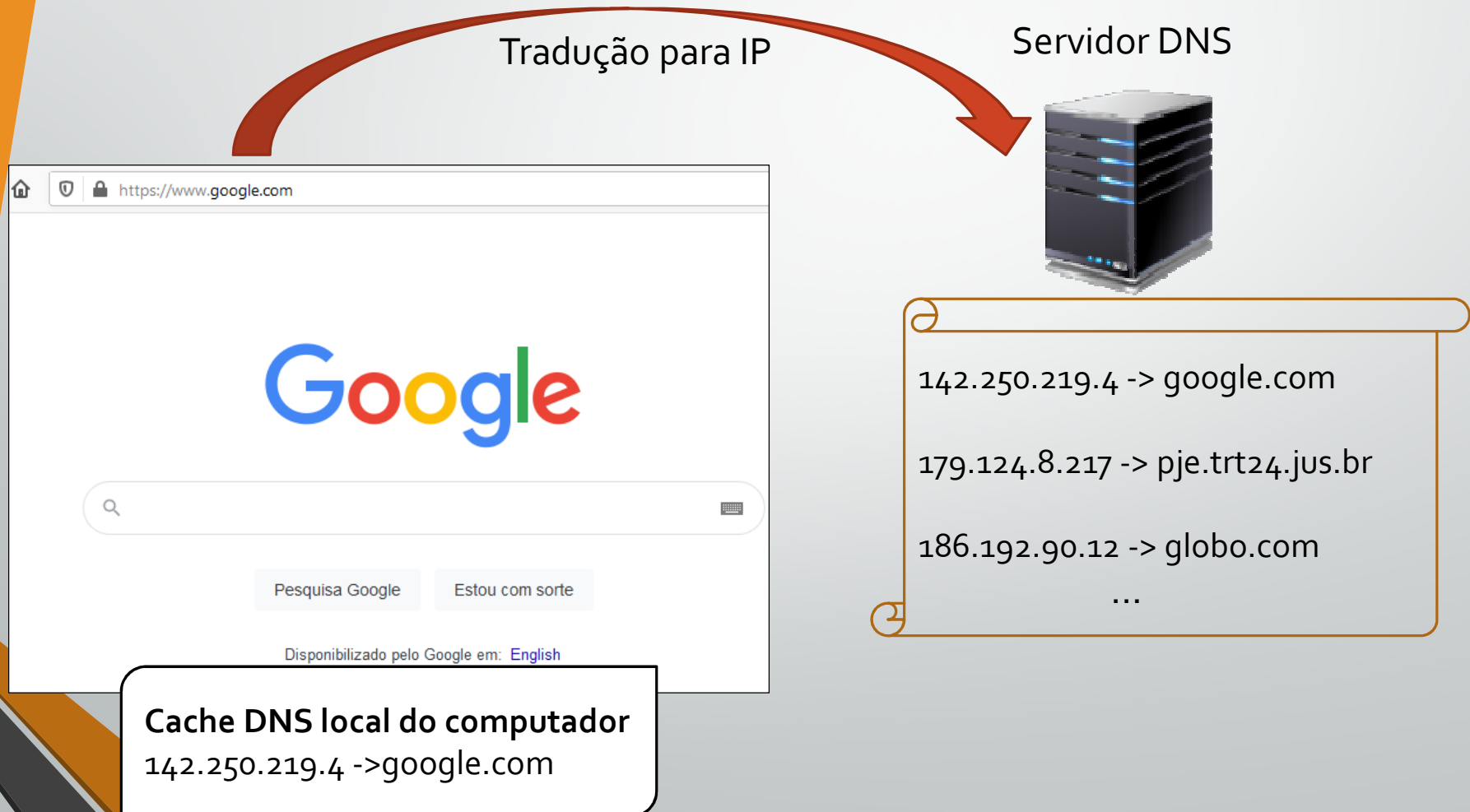
- Engenharia social

- 2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;

- DNS Poisoning – envenenamento de DNS



- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;
    - DNS Poisoning – envenenamento de DNS





- Engenharia social

- 2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;

- DNS Poisoning – envenenamento de DNS

Tradução para IP

Servidor DNS



142.250.219.4 -> google.com

179.124.8.217 -> pje.trt24.jus.br

186.192.90.12 -> globo.com

...

**Cache DNS local do computador**

142.250.219.4 -> google.com

179.124.8.217 -> pje.trt24.jus.br

- Engenharia social

- 2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;

- DNS Poisoning – envenenamento de DNS

Tradução para IP

Servidor DNS



142.250.219.4 -> google.com  
179.124.8.217 -> pje.trt24.jus.br  
186.192.90.12 -> globo.com  
...

Cache DNS local do computador

142.250.219.4 -> google.com  
184.171.14.88 -> pje.trt24.jus.br



- Engenharia social
  - 2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;
    - DNS Poisoning – envenenamento de DNS



**Cache DNS local do computador**  
142.250.219.4 -> google.com  
184.171.14.88 -> pje.trt24.jus.br

- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;
    - DNS Poisoning – envenenamento de DNS

## DNS Poisoning para finalizar o ataque

**De:** AdministradorPJe <[nao-responda@trt24-jus-br.com](mailto:nao-responda@trt24-jus-br.com)>  
**Data:** 28 de outubro de 2021 13:43:12 AMT  
**Para:** <[fabio.nogueira86@gmail.com](mailto:fabio.nogueira86@gmail.com)>  
**Assunto:** Altere o PIN do seu token para não perder o acesso ao PJe



Prezado usuário,

Estamos modificando nosso modelo de autenticação para melhor atendê-lo e trazer mais segurança ao nosso sistema. Pedimos, por gentileza, que altere o número PIN do seu certificado para atendimento à política de alteração de senhas. Segue link para acesso rápido:

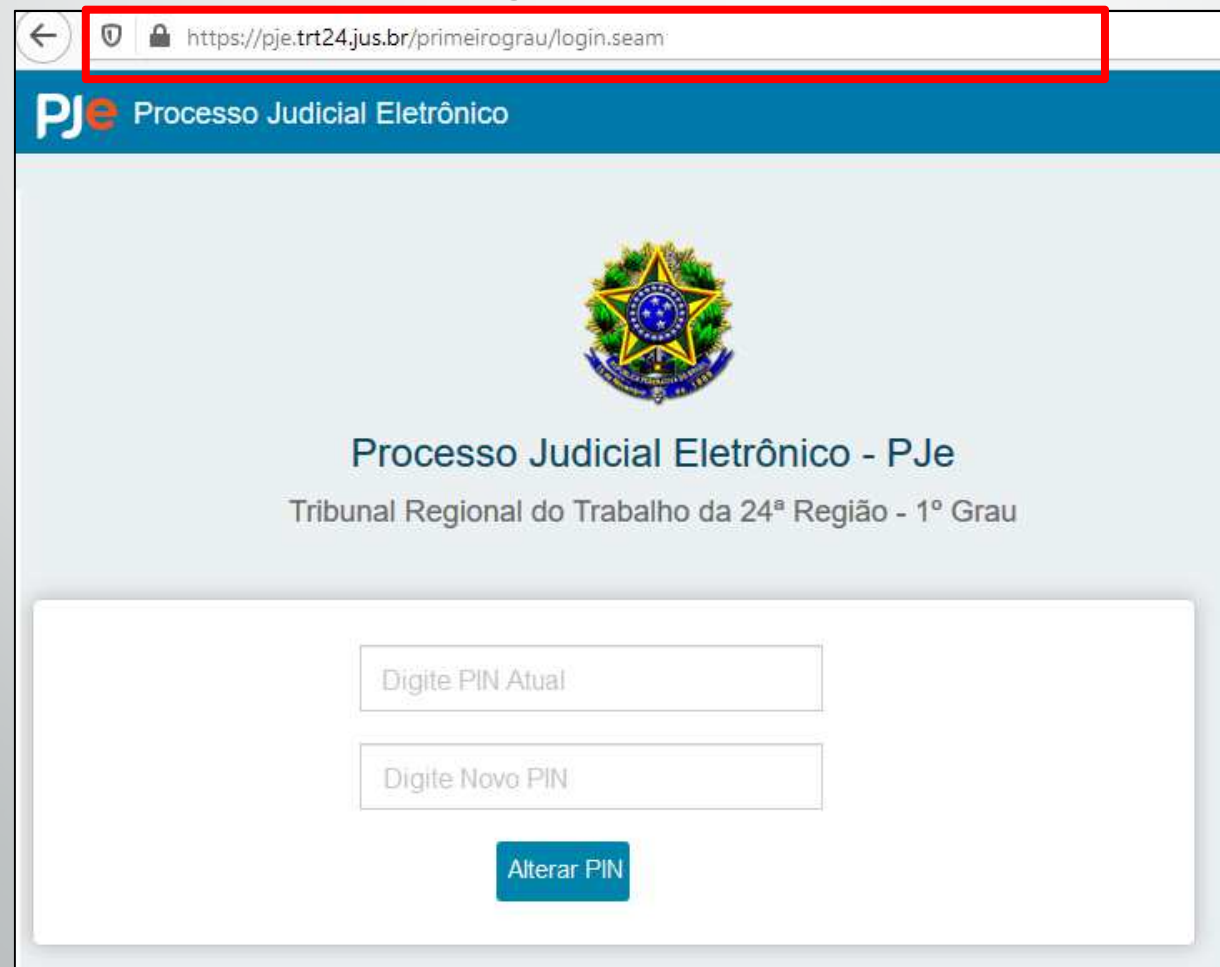
<https://pje.trt24.jus.br/primeirograu/login.seam>

Atenciosamente:

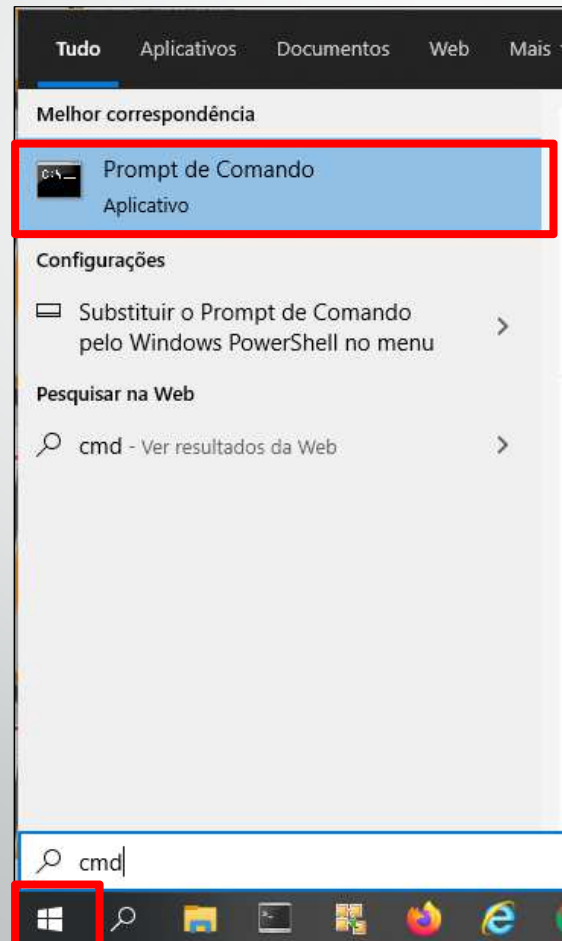
Equipe de TI do TRT24|

- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;
    - DNS Poisoning – envenenamento de DNS

### DNS Poisoning para finalizar o ataque



- Engenharia social
  - 2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;
    - DNS Poisoning – envenenamento de DNS: como verificar se estou contaminado ?





- Engenharia social

- 2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;

- DNS Poisoning – envenenamento de DNS: como verificar se estou contaminado?

```
Administrator: Prompt de Comando - ping pje.trt24.jus.br  
  
C:\Users\sausinf>ping pje.trt24.jus.br  
  
Disparando pje.trt24.jus.br [179.124.8.217] com 32 bytes de dados:  
Esgotado o tempo limite do pedido.  
Esgotado o tempo limite do pedido.  
  
-
```

- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;
    - DNS Poisoning – envenenamento de DNS: como verificar se estou contaminado?
      - 8.8.8.8 é o endereço IP do DNS do google, de conhecimento público na Internet

```
C:\Users\sausinf>nslookup pje.trt24.jus.br 8.8.8.8
Servidor:  dns.google
Address:  8.8.8.8

Não é resposta autoritativa:
Nome:      pje.trt24.jus.br
Address:   179.124.8.217

C:\Users\sausinf>
```

- Engenharia social
  2. XSS, injeções e “DNS Poisoning”: Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;
    - DNS Poisoning – envenenamento de DNS: como verificar se estou contaminado?

```
C:\> Administrador: Prompt de Comando - ping pje.trt24.jus.br
```

```
C:\Users\sausinf> ping pje.trt24.jus.br
```

```
Disparando pje.trt24.jus.br [179.124.8.217] com 32 byte  
Esgotado o tempo limite do pedido.
```

```
C:\> Administrador: Prompt de Comando
```

```
C:\Users\sausinf> nslookup pje.trt24.jus.br 8.8.8.8
```

```
Servidor: dns.google
```

```
Address: 8.8.8.8
```

```
Não é resposta autoritativa:
```

```
Nome: pje.trt24.jus.br
```

```
Address: 179.124.8.217
```

- ## Contra medidas

1. Phishing;

2. XSS, injeções e "DNS Poisoning"

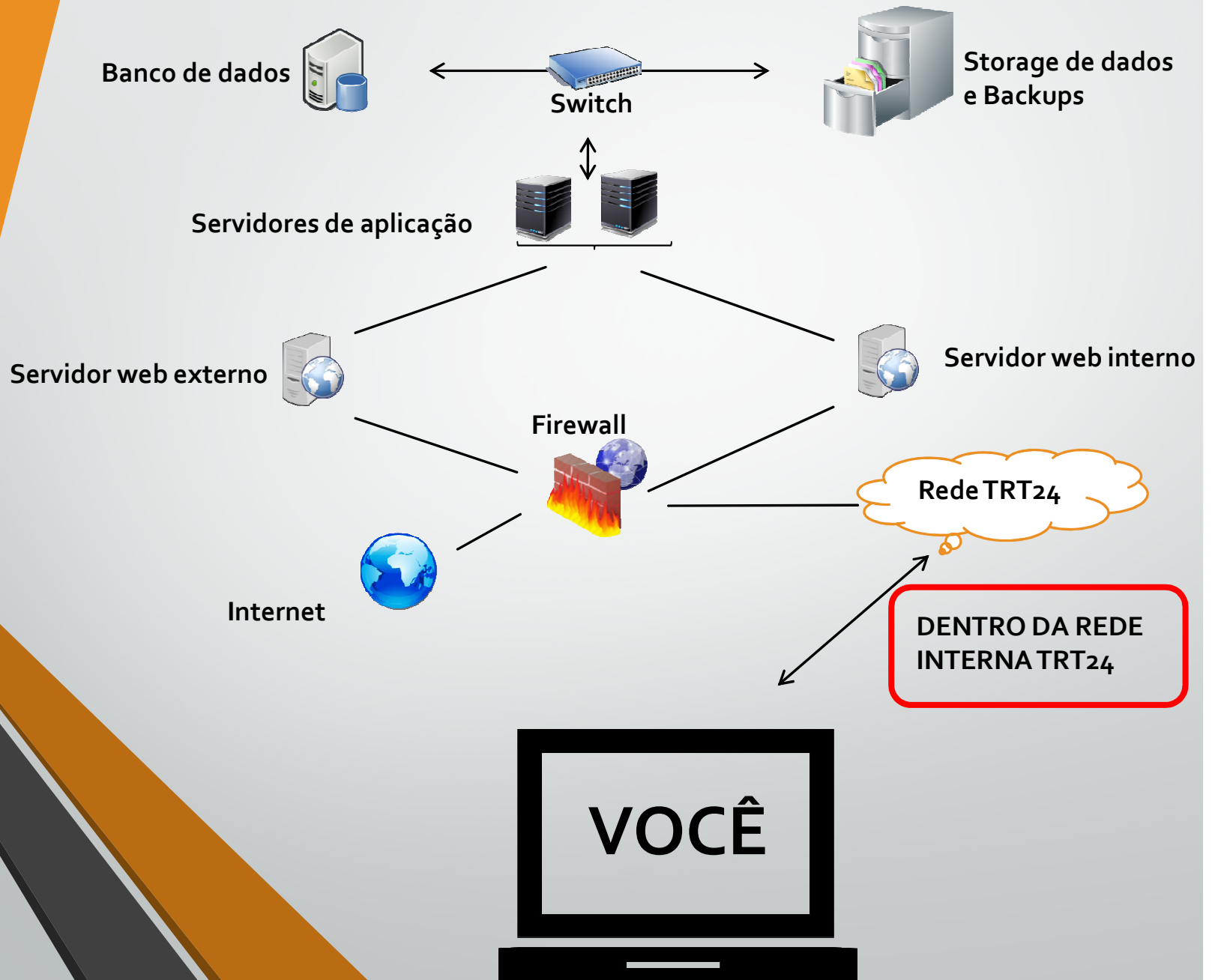
- ✓ Evite sempre clicar em links de e-mails. Prefira acessar o site manualmente no navegador;
- ✓ Faça as verificações ensinadas aqui sempre que desconfiar de algo (whois, receita federal, dns do google)
- ✓ Desconfie sempre que a aplicação utilizada por você solicitar informações confidenciais que nunca foram pedidas antes;
- ✓ Evite acessar sites desconhecidos ou estranhos. Pode ser possível ataque XSS só de entrar nesse tipo de site;
- ✓ Utilize os computadores do TRT somente para acesso a sites relacionados ao trabalho;

# Principais ataques à Segurança da Informação e contramedidas

- Engenharia social
  3. Ransoware – Sequestro de informação;

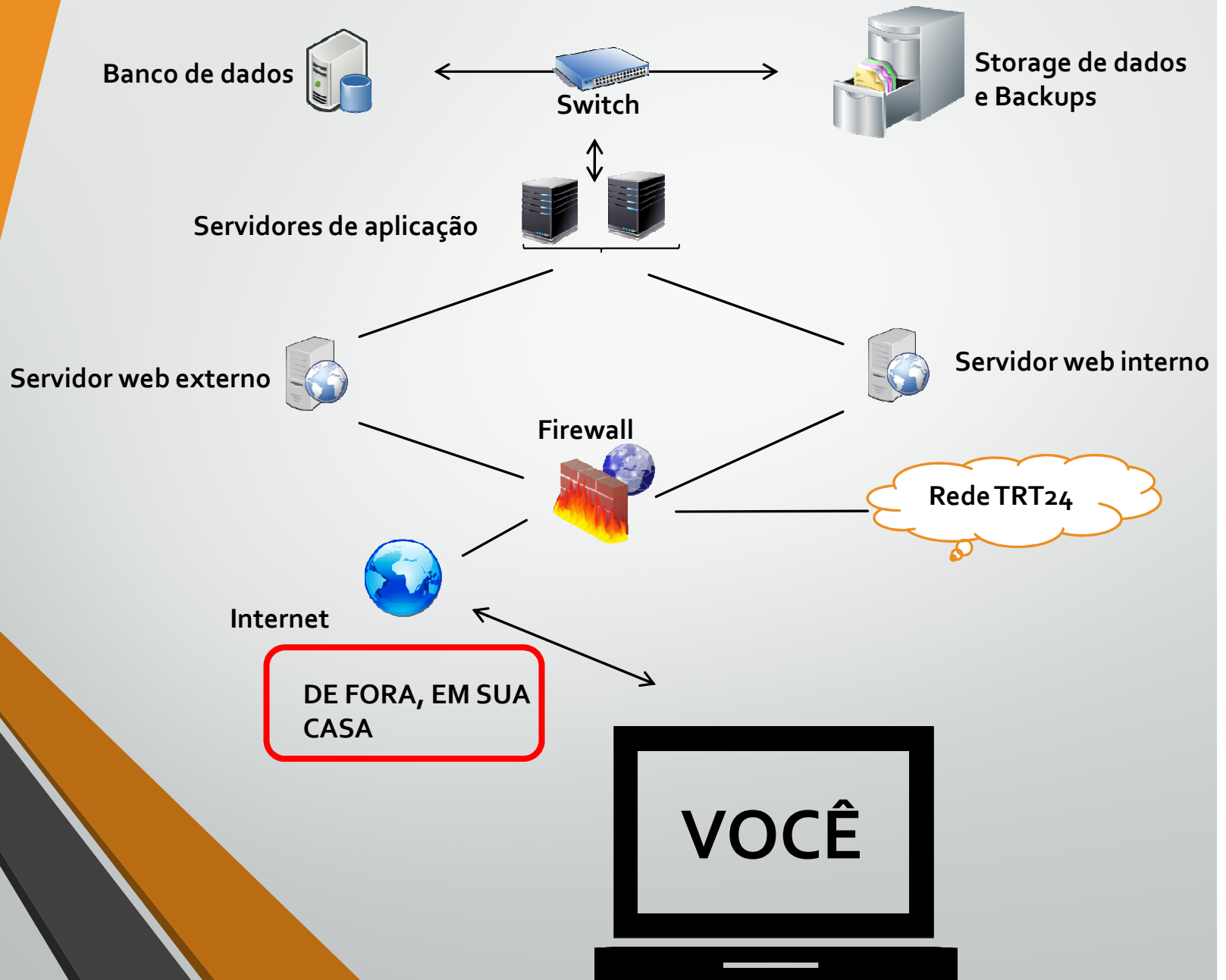


# Ransomware – contaminação

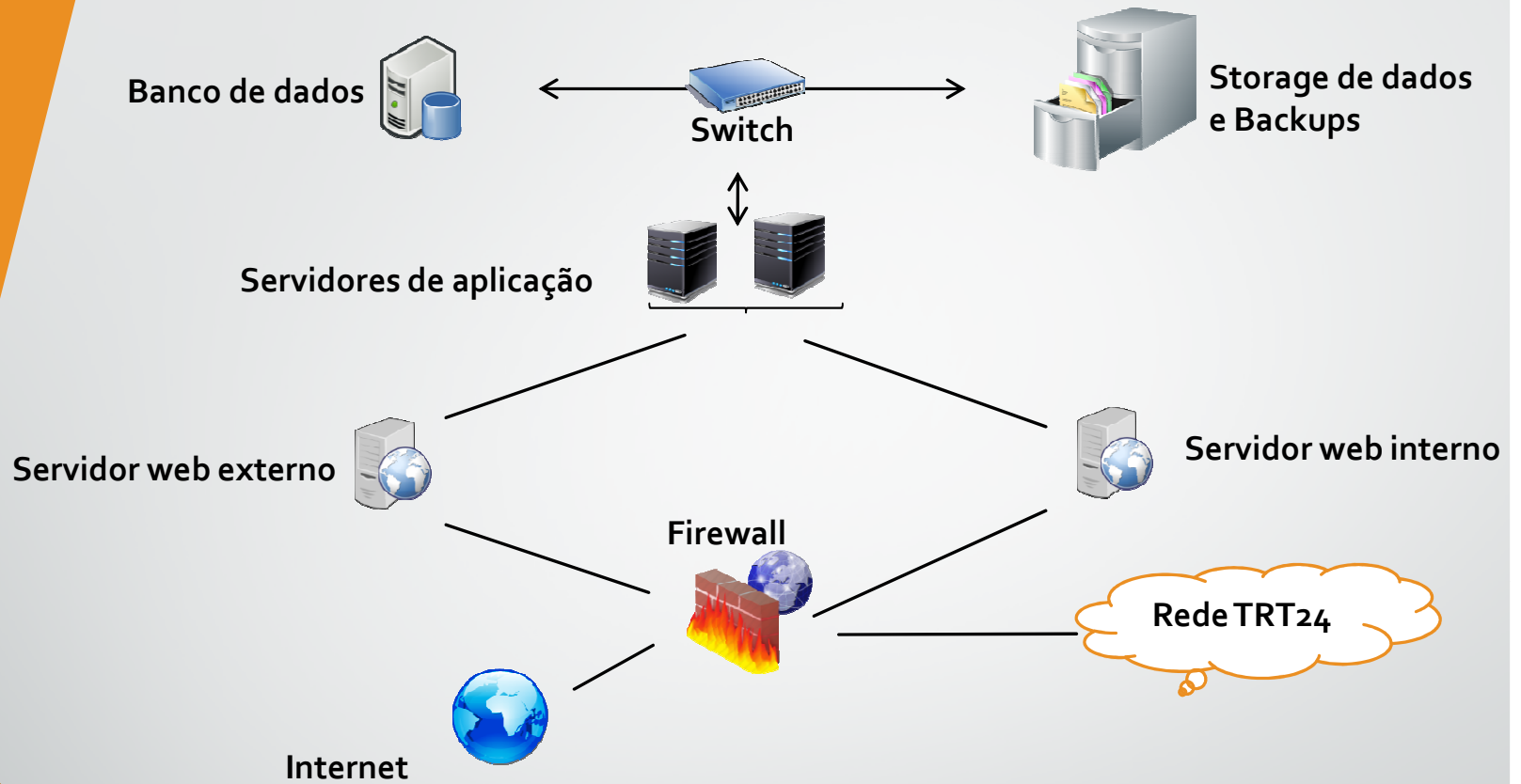




# Ransomware – contaminação



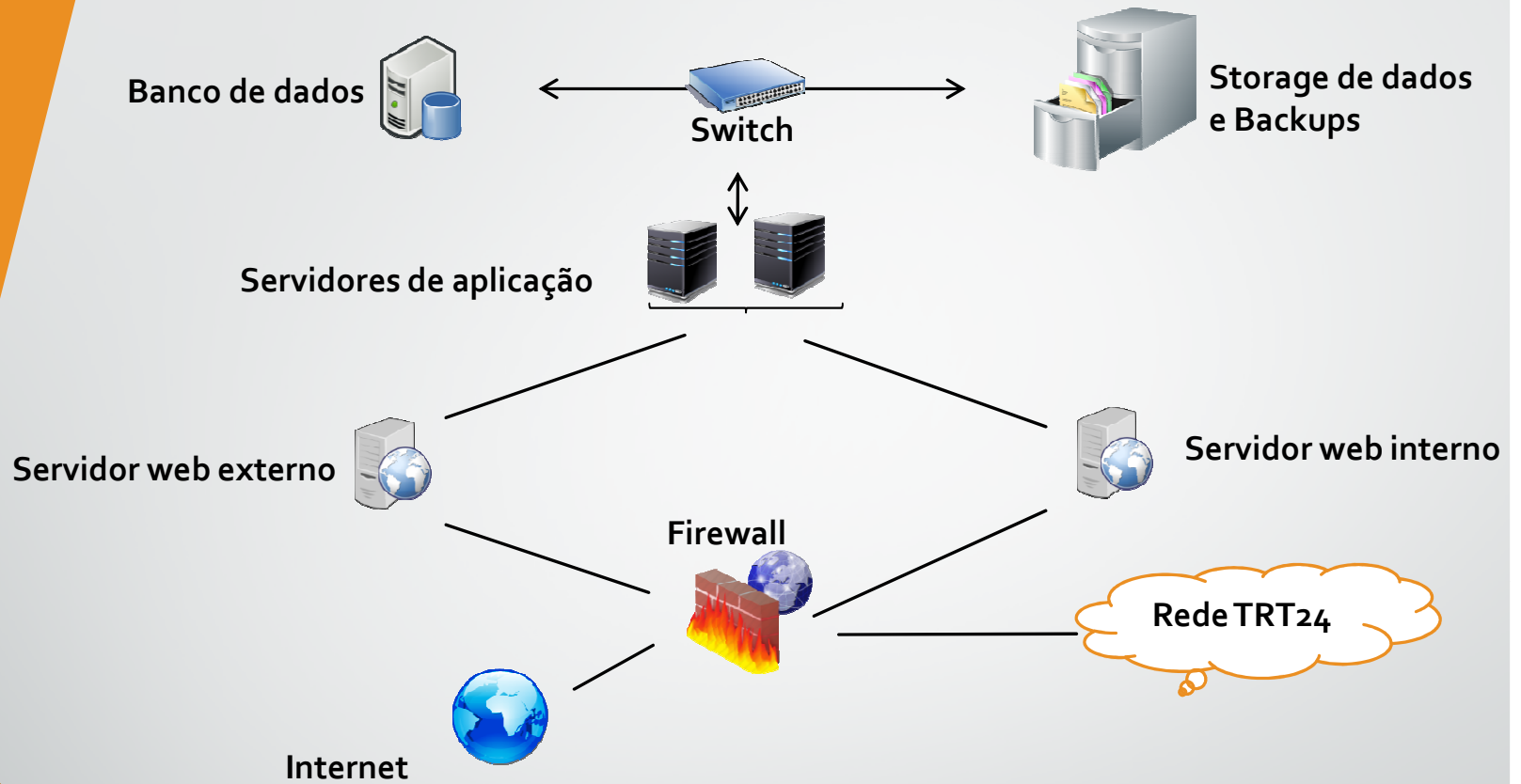
# Ransomware – contaminação



NÃO VERIFICAR SE  
ANTIVÍRUS E WINDOWS  
ESTÃO COM AS ÚLTIMAS  
ATUALIZAÇÕES



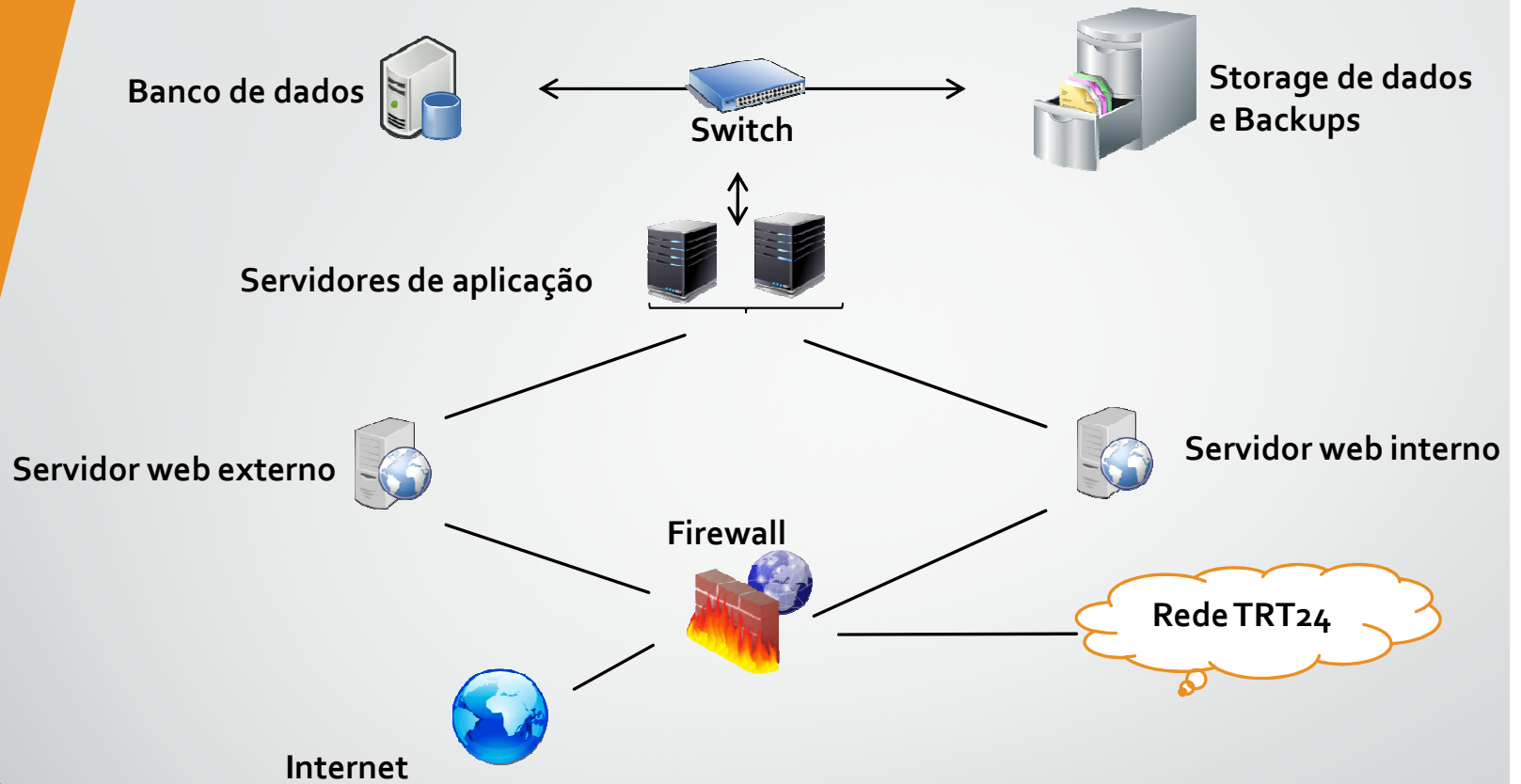
# Ransomware – contaminação



CLICAR EM LINKS E ANEXOS DE EMAILS CONTAMINADOS



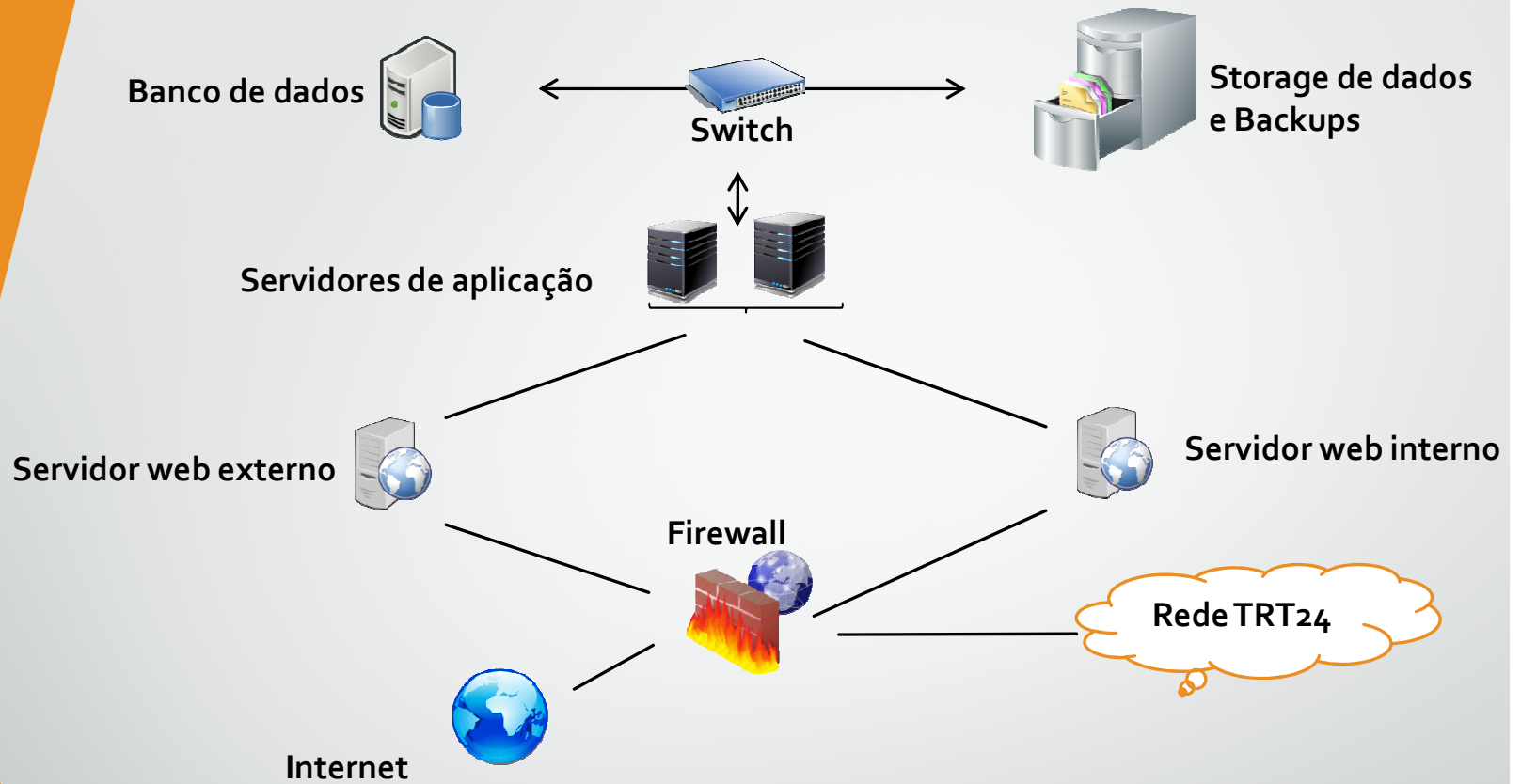
# Ransomware – contaminação



BAIXAR E EXECUTAR  
ARQUIVOS  
CONTAMINADOS DE  
SITES INSEGUROS



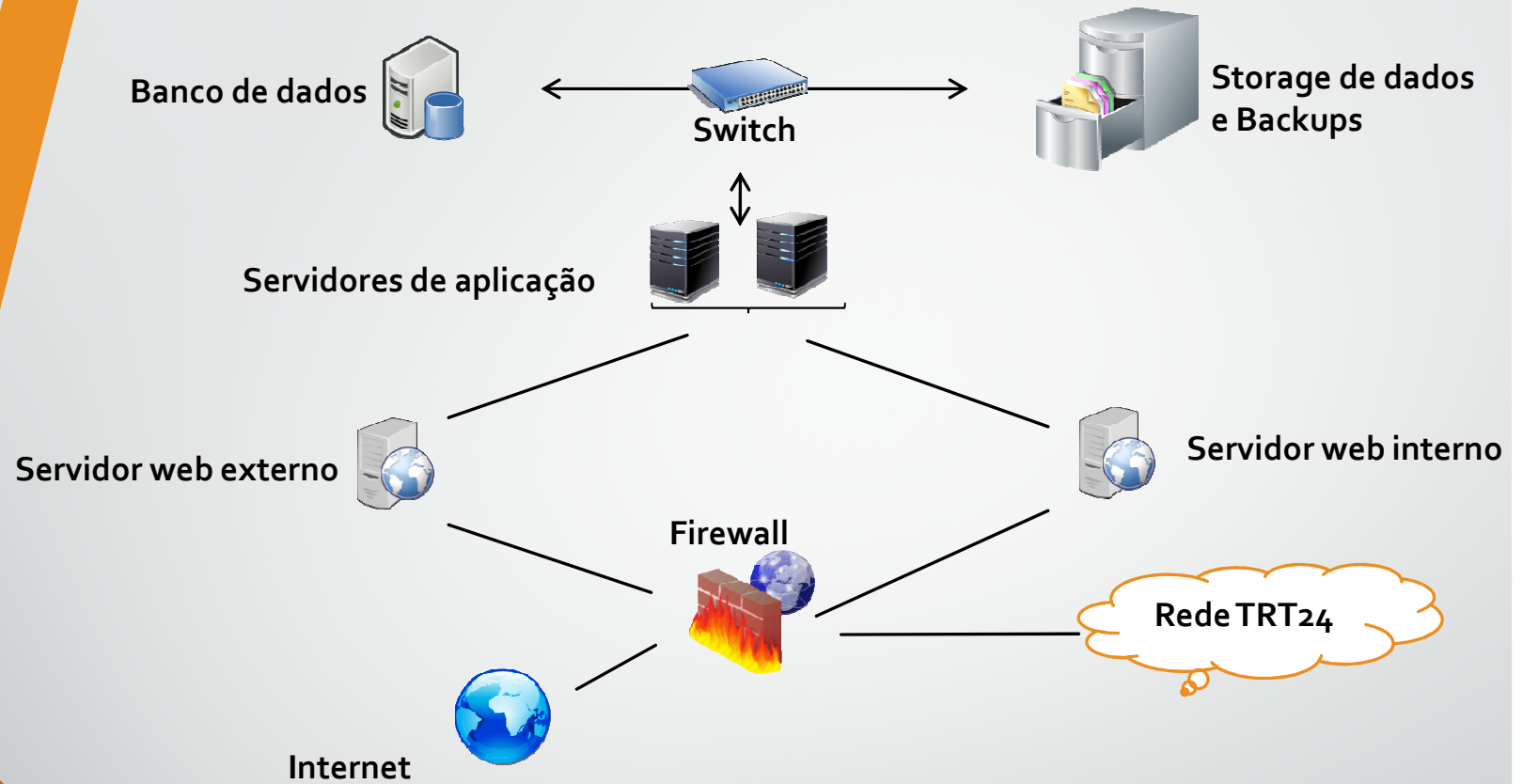
# Ransomware – contaminação



INSTALAR SOFTWARES  
SEM  
ACOMPANHAMENTO  
DA TI



# Ransomware – contaminação

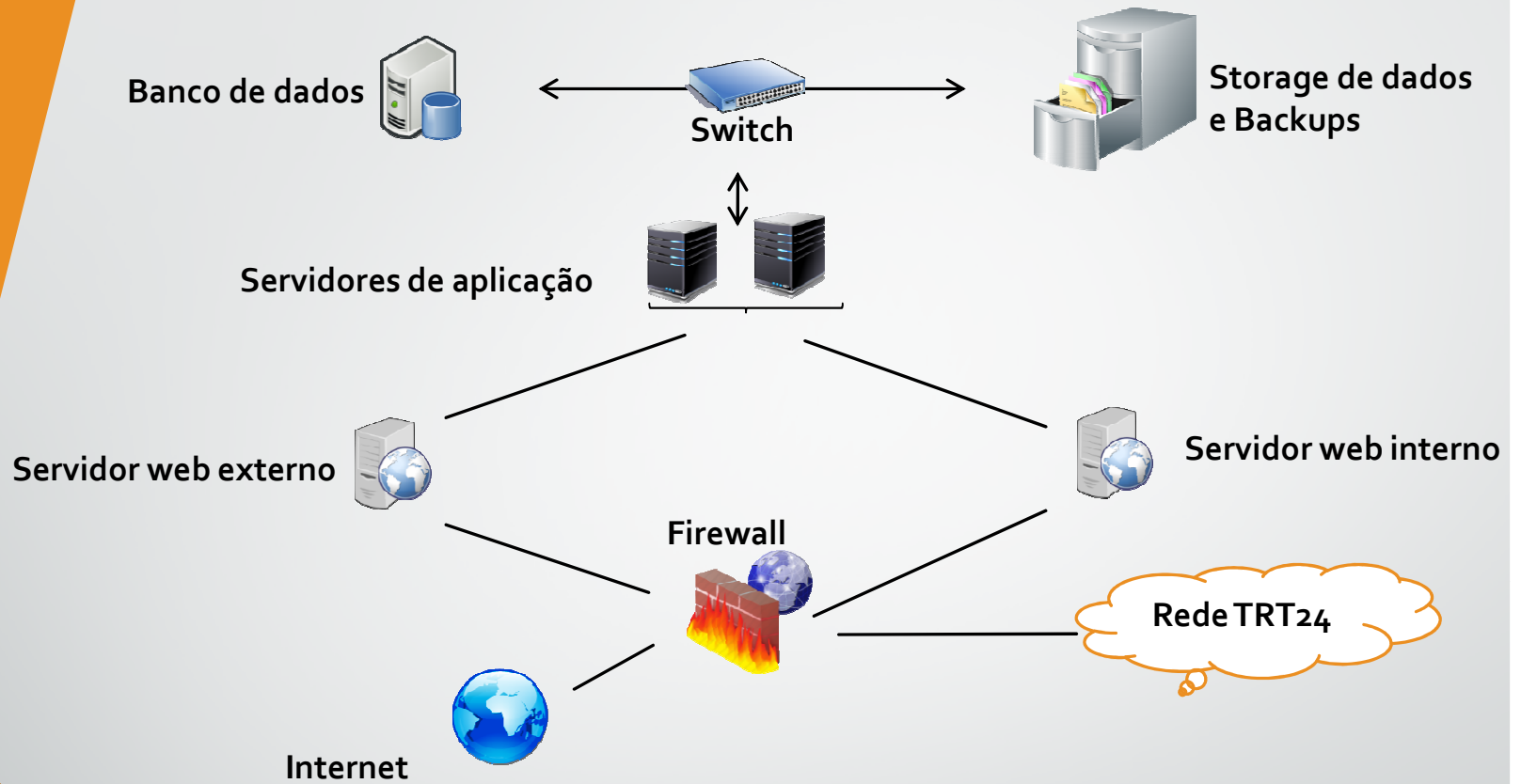


DESATIVAR O  
ANTIVÍRUS POR CONTA  
PRÓPRIA





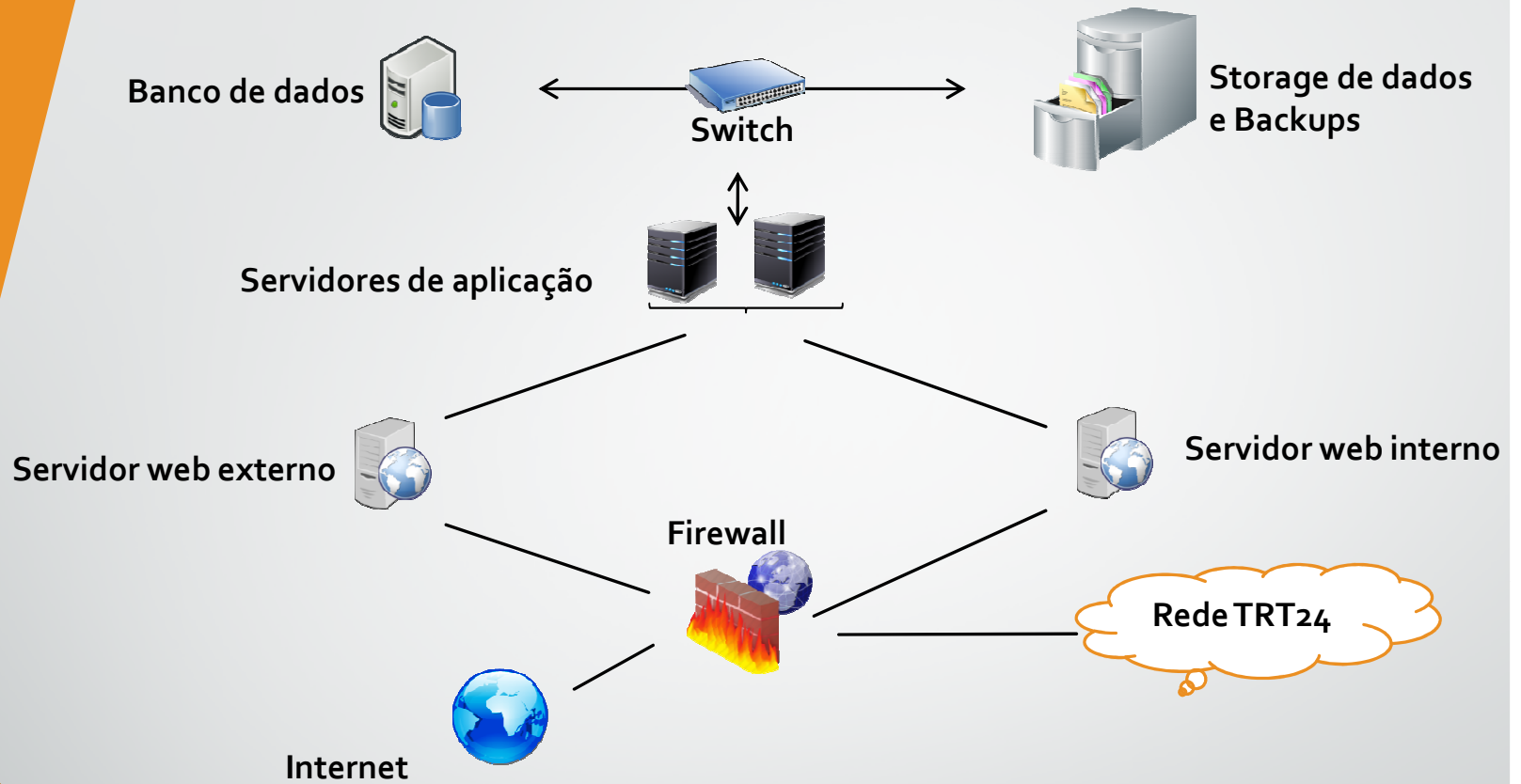
# Ransomware – contaminação



NÃO UTILIZAR SENHAS  
FORTES PARA O SEU  
LOGIN



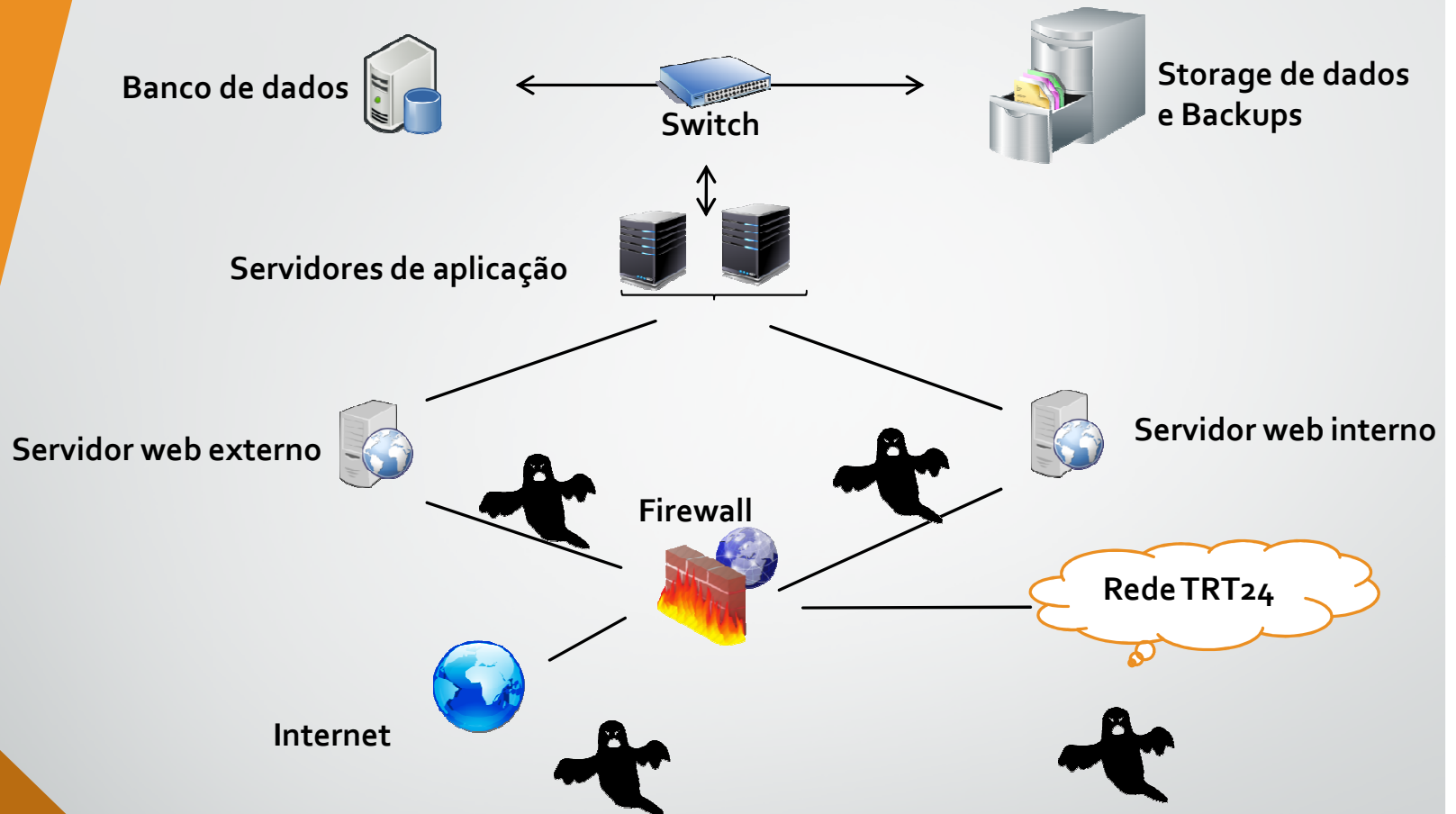
# Ransomware – contaminação



**RANSOWARE  
CRIPTOGRAFA DADOS  
LOCAIS DA SUA  
ESTAÇÃO**



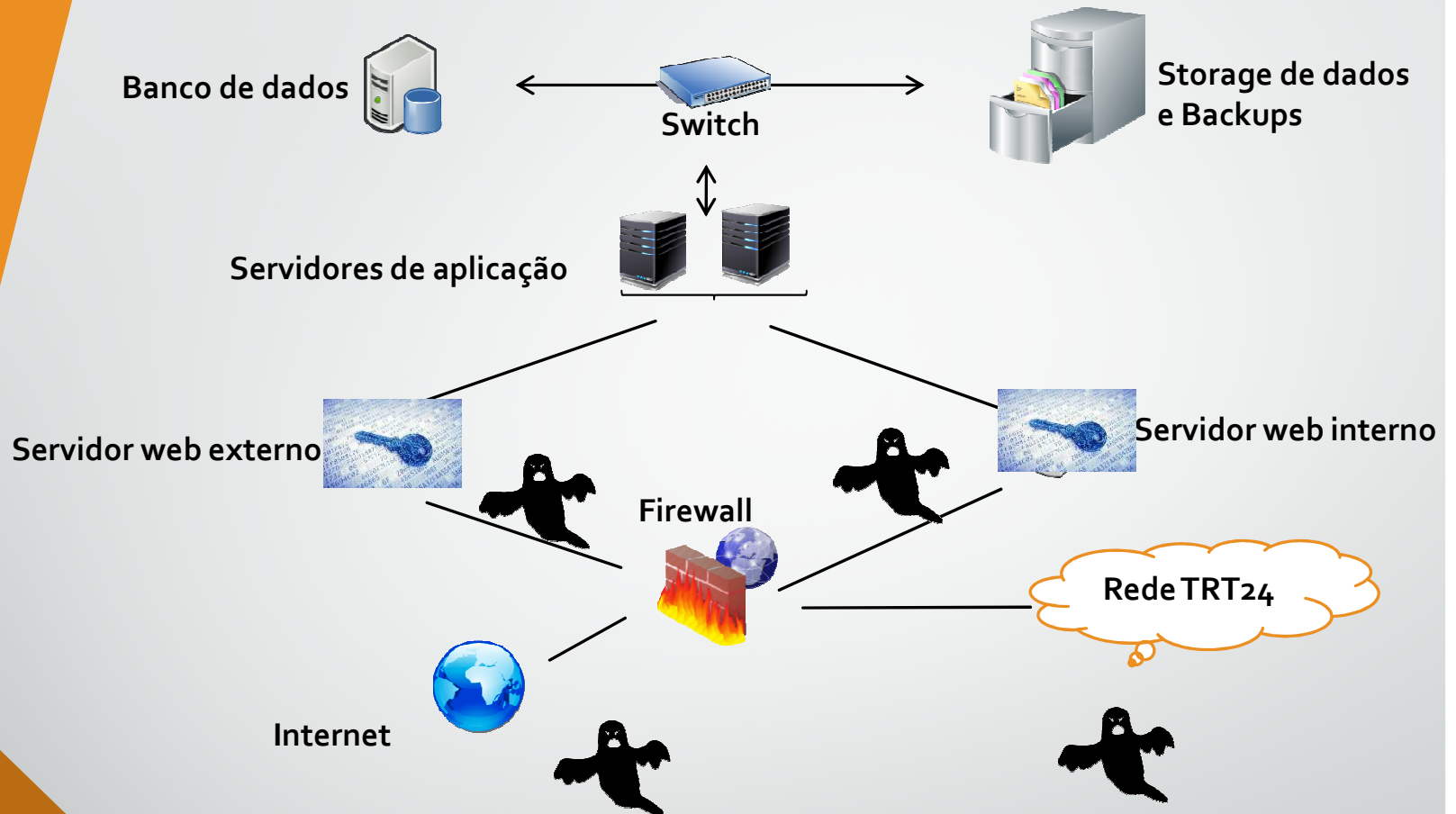
# Ransomware – contaminação



**RANSOWARE SE PROPAGA PELA REDE ATRAVÉS DE ALGUMA VULNERABILIDADE SEM ATUALIZAÇÃO**



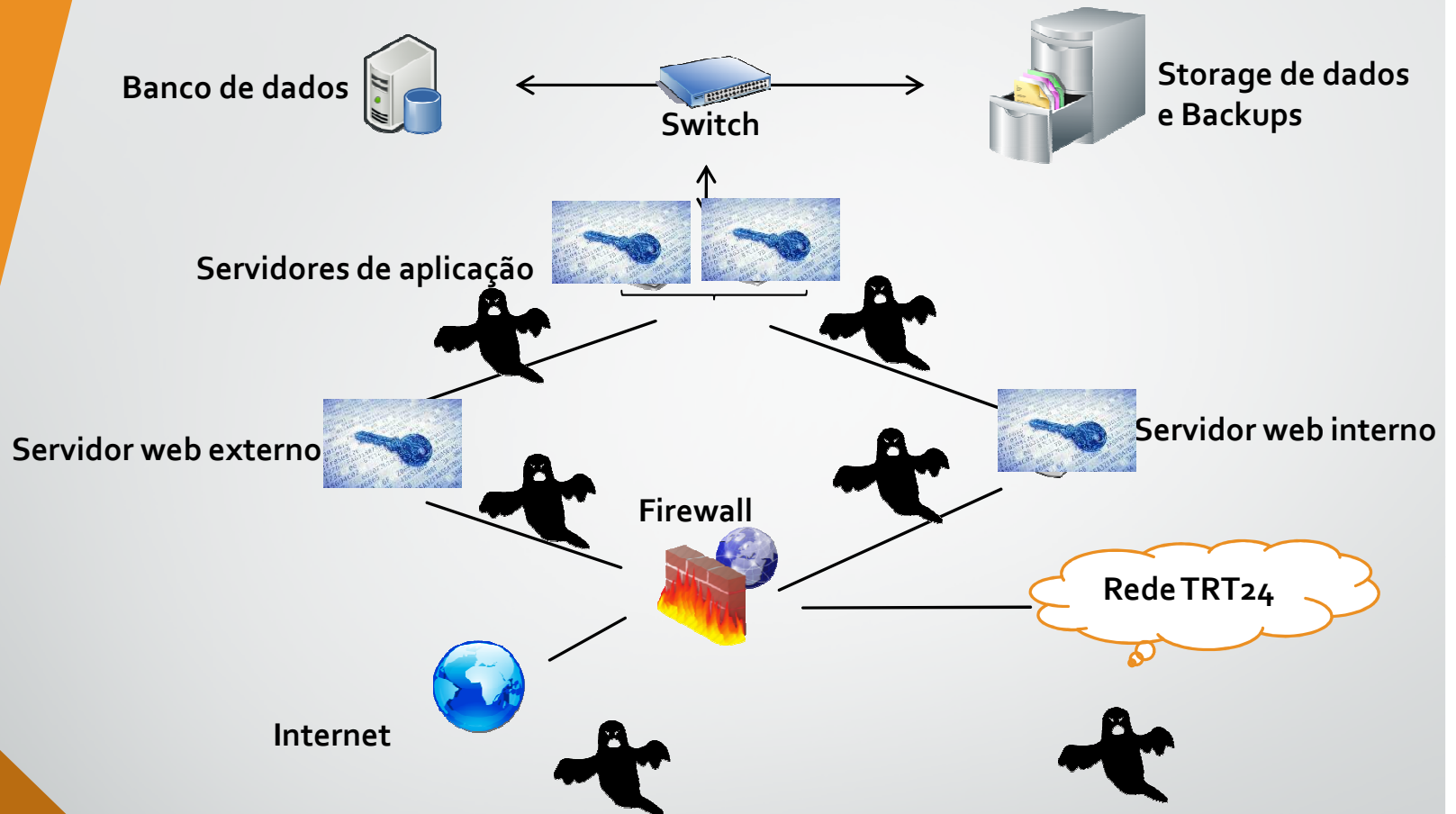
# Ransomware – contaminação



**RANSOWARE VAI  
CRIFTOGRAFANDO OS  
DADOS DOS ATIVOS  
PELO CAMINHO**



# Ransomware – contaminação

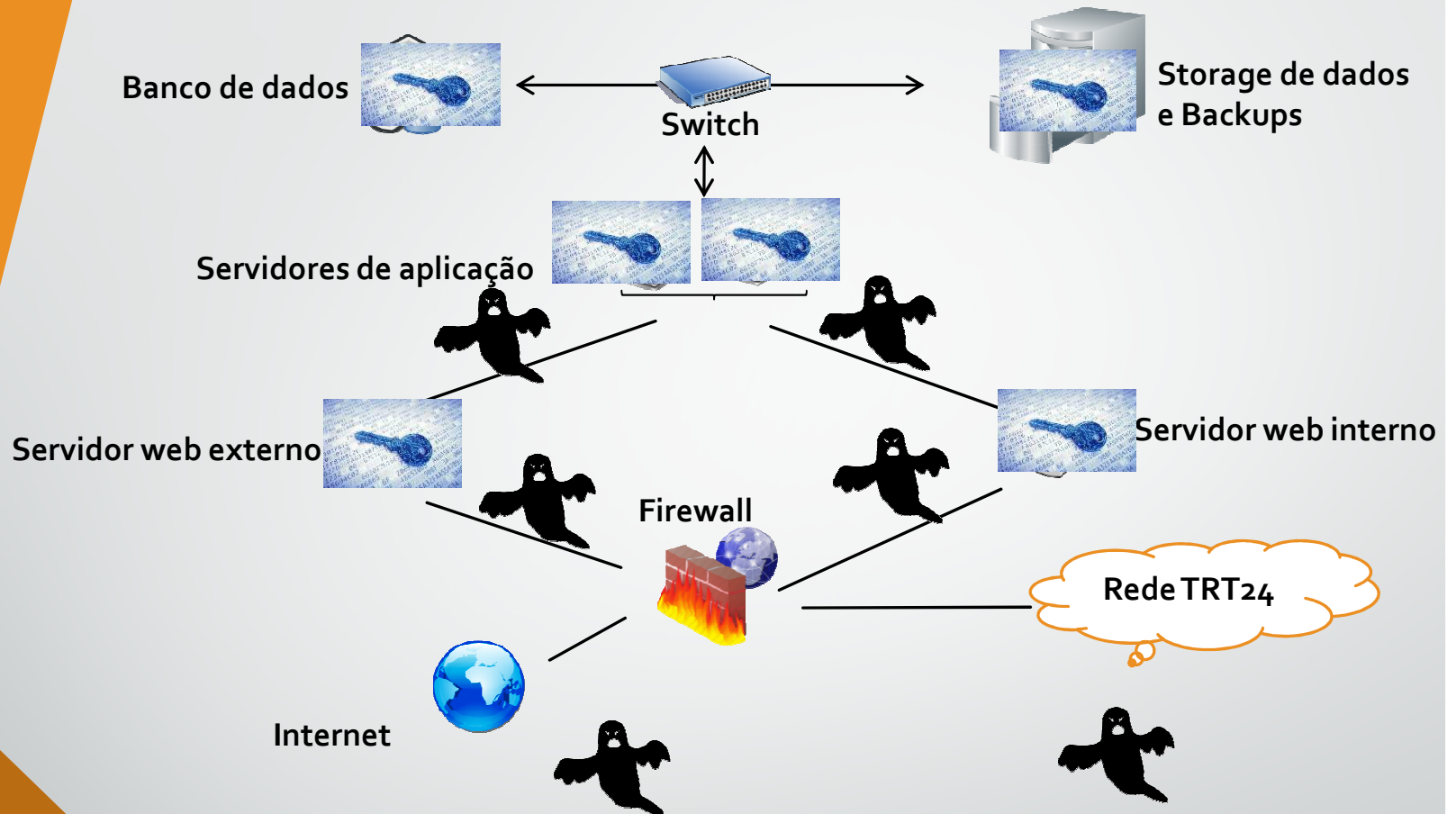


**QUANTO MAIS SE PROPAGA, PIOR VAI FICANDO O CENÁRIO.**





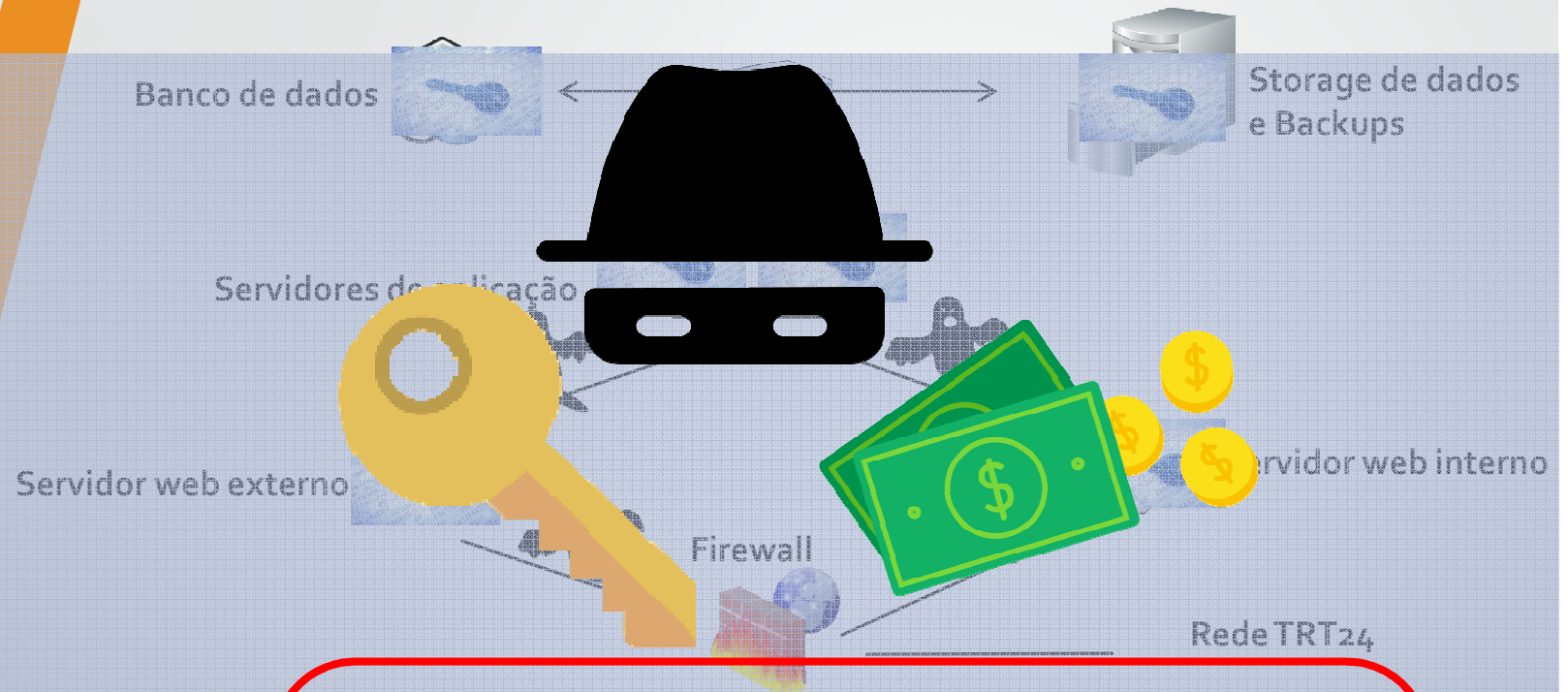
# Ransomware – contaminação



**NO PIOR DOS CASOS,  
PODE ATINGIR O  
SERVIDOR DE  
BACKUPS,  
DIFICULTANDO A  
RESTAURAÇÃO DOS  
DADOS**



# Ransomware – contaminação



-NO FINAL DE TUDO, O ATACANTE PEDE RESGATE EM TROCA DA CHAVE CAPAZ DE RECUPERAR AS INFORMAÇÕES.

-VALORES VARIAM DE 5 MIL a 40 MILHÕES DE DÓLARES.

-MESMO PAGANDO O VALOR, APENAS 1/3 DOS ATACANTES ENTREGAM A CHAVE DE DESEMBARALHAMENTO.

-ESSE TIPO DE ATAQUE AUMENTOU 62% SÓ NO ANO PASSADO.



# Ransomware – contaminação



**-APÓS UM EVENTO DESSE TIPO, OS DANOS À IMAGEM DA INSTITUIÇÃO PODEM SER IRREPARÁVEIS.**

**-DEVIDO AO GRANDE IMPACTO QUE CAUSA, DEVEMOS ACEITAR A DIMINUIÇÃO DO GRAU DE FLEXIBILIDADE QUE AS MEDIDAS DE SEGURANÇA TRARÃO NO SEU DIA A DIA.**

# Principais ataques à Segurança da Informação e contramedidas

- Engenharia social
  - 4. Quebra de senhas:
    - Ataque força bruta - senhas fracas;
    - Ataques de dicionário – senhas fracas;

- Engenharia social

- 4. Quebra de senhas: **Ataque de força bruta - senhas fracas**

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

- Engenharia social

- 4. Quebra de senhas: **Ataque de força bruta** - senhas fracas - contramedidas:

- Utilizar senhas fortes

- Tamanho mínimo 8 caracteres;
      - Possuir letras e números não sequenciais;
      - Possuir pelo menos 1 letra maiúscula ou minúscula;
      - Ter pelo menos um dos seguintes caracteres especiais:  
@ ! # \$ % &
      - Não possuir informações pessoais;
      - Não anotar em papel;

- Autenticação multifator – combinação de 2 ou mais métodos de autenticação de classes diferentes:

- O que você sabe: senha, perguntas pessoais, etc;
      - O que você é: biometria, digital, etc;
      - O que você tem: smart cards, tokens, etc;

- Engenharia social

- 4. Quebra de senhas: **Ataque de força bruta** - senhas fracas - contramedidas:

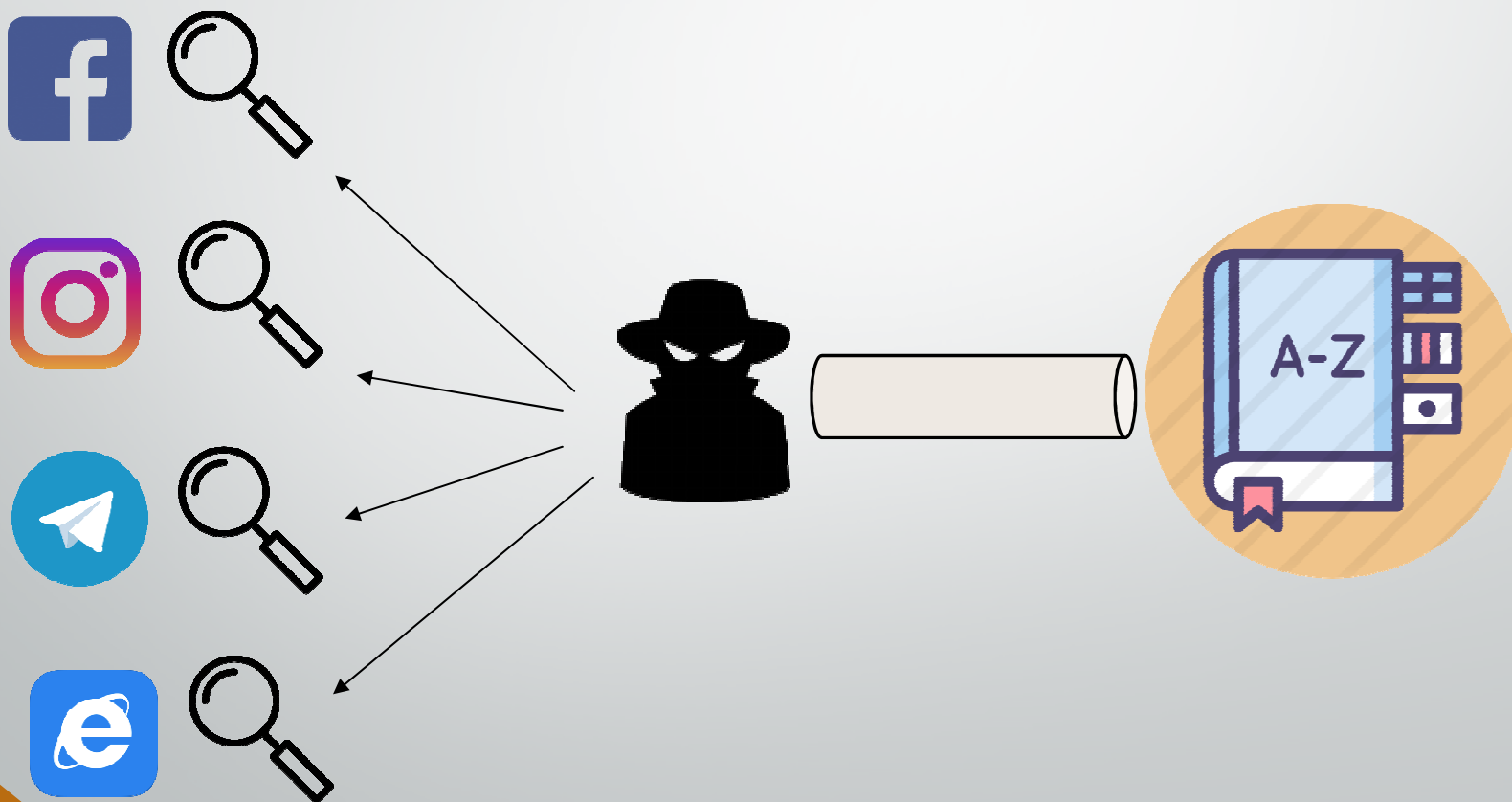
- Método para confeccionar senhas fortes:

- Escolha uma frase da qual goste: "Penso logo existo"
      - Escolha um número do qual goste: 6
      - Escolha um caractere especial: @
      - Posicione o número escolhido nos espaços da frase escolhida e coloque o caractere especial no último espaço. Nova senha ficaria:

**Penso6logo@existo**

- Engenharia social

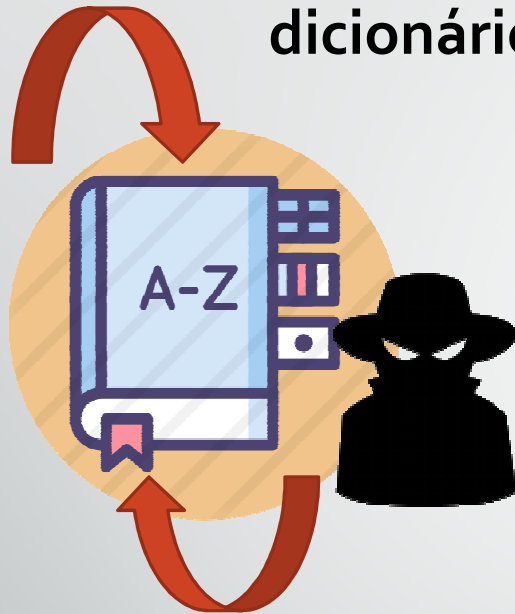
- 4. Quebra de senhas: **Ataque de dicionário - senhas fracas**





- Engenharia social

- 4. Quebra de senhas: **Ataque de dicionário - senhas fracas**

A screenshot of a login form. It features two input fields: the top one is labeled 'CPF' and the bottom one is labeled 'Senha'. Below the 'Senha' field is a blue link that says 'Esqueci minha senha'. At the bottom right of the form is a blue button with the text 'ENTRAR' in white capital letters.



- Engenharia social

- 4. Quebra de senhas: **Ataque de dicionário – contramedidas**

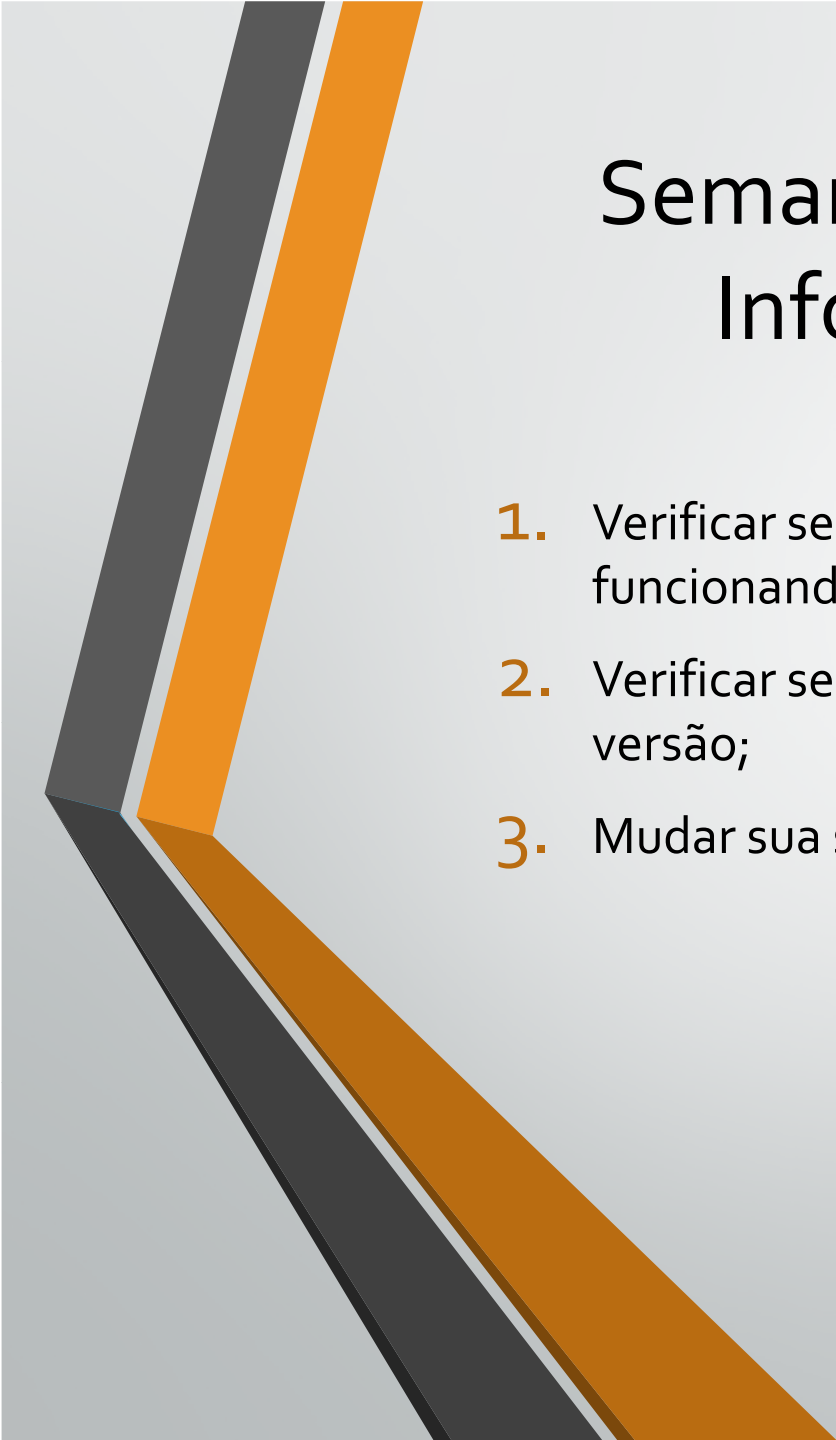
- Manter informações pessoais em modo privado nas redes sociais e Internet em geral;
    - Evite falar do seu trabalho em redes sociais ou fóruns de discussão;
    - Não passe suas informações pessoais por telefone;
    - Senha do TRT diferente das senhas utilizadas em redes sociais ou outros sites;

# Semana da Segurança da Informação – parte II

- Considerando-se o retorno das atividades presenciais no dia 08/11/2021;
- Considerando-se a **baixa adesão** dos colaboradores do TRT24 na primeira Semana de Segurança da Informação;
- Considerando-se que os **ATAQUES** à segurança da informação não param de **CRESCER**;

# Semana da Segurança da Informação – parte II

- Ficou definido, pelo Comitê Técnico de Segurança da Informação do TRT24, uma **série de ações** que, **caso não cumpridas**, causarão o **BLOQUEIO da Internet** nos computadores alvos **a partir do dia 29/11/2021**
- Serão **3 semanas** para que os colaboradores do TRT24 acompanhem e verifiquem se suas máquinas atendem aos requisitos de Segurança;



# Semana da Segurança da Informação - Ações

1. Verificar se o seu antivírus está atualizado e funcionando;
2. Verificar se o seu Windows está atualizado e na última versão;
3. Mudar sua senha na Intranet a partir de abril/maio 2022;

# Semana da Segurança da Informação – Ações

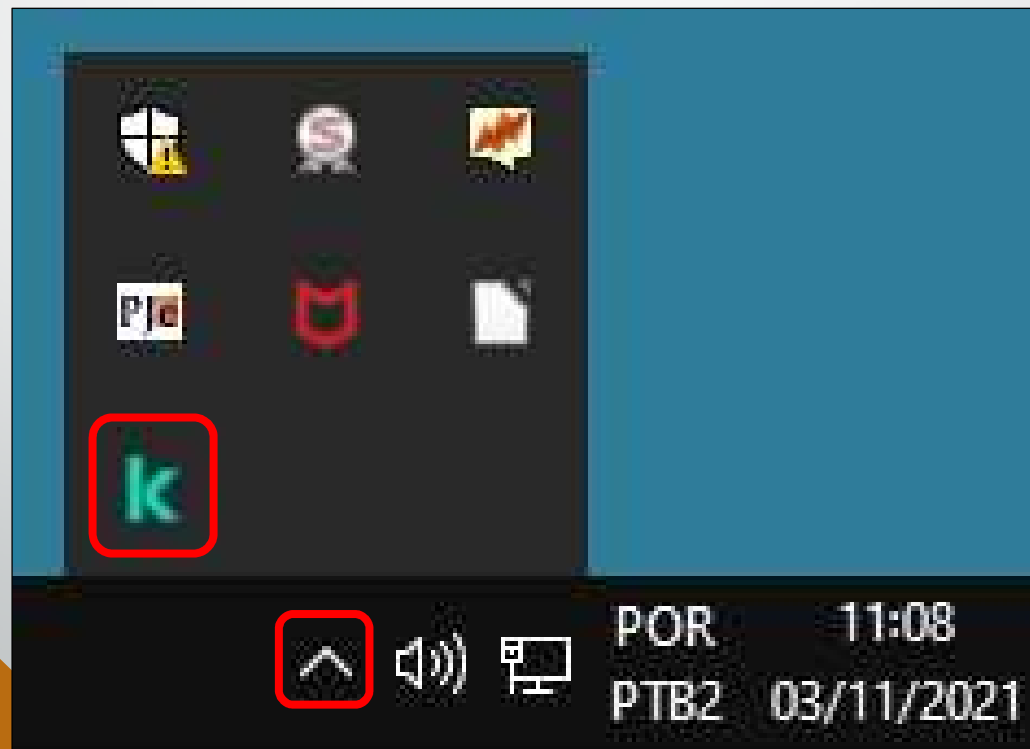
1. Verificar se o seu antivírus está atualizado e funcionando (Rede interna TRT24)
  - A partir do dia 09/11/2021, iniciaremos o processo de migração de antivírus da **Mcafee** para a solução recém adquirida da **Kaspersky**;
  - Muito importante que todas as máquinas estejam ligadas e logadas para que o processo ocorra com sucesso;
  - Só desliguem as máquinas caso o antivírus da Kaspersky esteja corretamente instalado;

# Semana da Segurança da Informação – Ações

1. Verificar se o seu antivírus está atualizado e funcionando (Fora do TRT24 – teletrabalho ordinário)
  - Caso a máquina pertença ao TRT24, **abrir SIATE** para instalação manual do agente de comunicação da Kaspersky e remoção do antigo antivírus;
  - Verificar, no período de 09/11/2021 a 29/11/2021, se o antivírus Kaspersky foi corretamente instalado;

# Semana da Segurança da Informação – Ações

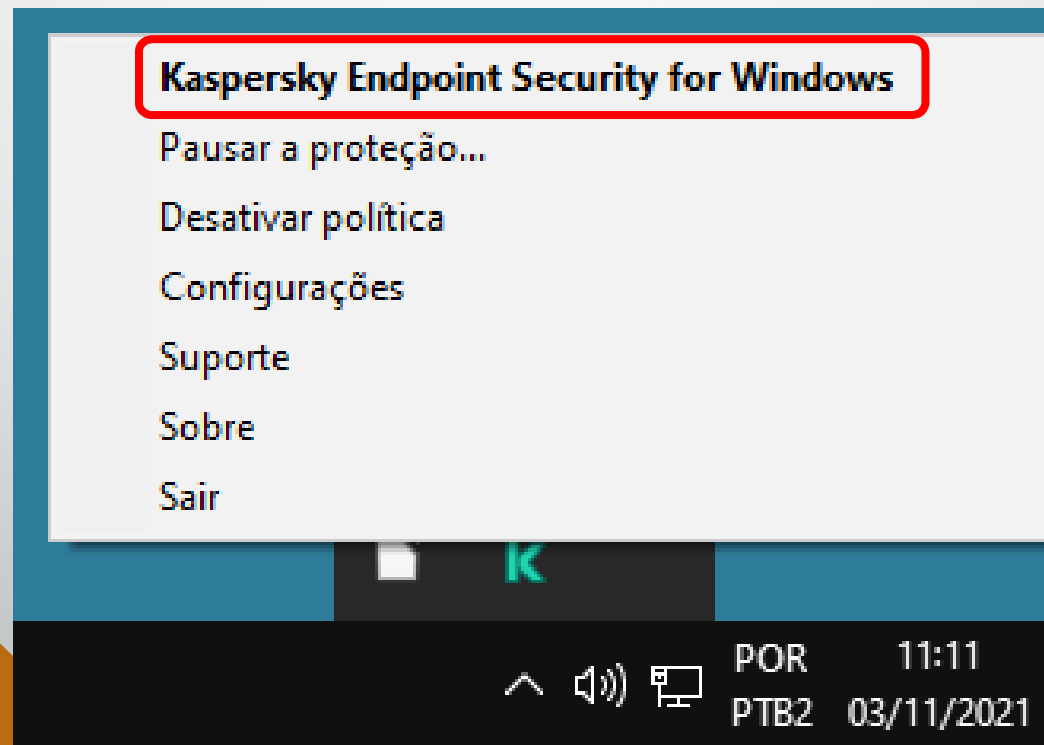
1. Verificar se o seu antivírus está atualizado e funcionando
  - Como verificar se o Kaspersky está instalado e atualizado na sua máquina ?





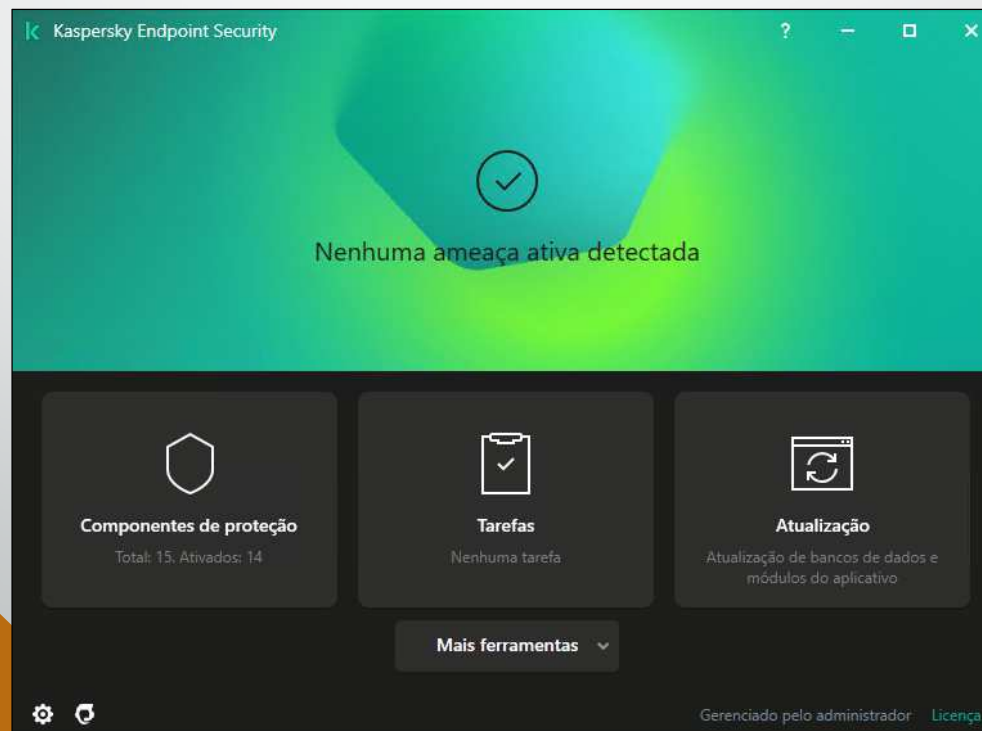
# Semana da Segurança da Informação – Ações

1. Verificar se o seu antivírus está atualizado e funcionando
  - Como verificar se o Kaspersky está instalado e atualizado na sua máquina ?



# Semana da Segurança da Informação – Ações

1. Verificar se o seu antivírus está atualizado e funcionando
  - Como verificar se o Kaspersky está instalado e atualizado na sua máquina ? **Abrir SIATE imediatamente** caso algo seja detectado;



# Semana da Segurança da Informação – Ações

2. Verificar se o seu Windows está atualizado e na última versão;



- Deixe o seu computador ligado e reinicie quando solicitado pelo Windows;
- O processo de atualização é lento devido ao tamanho dos pacotes. Verifique diariamente se seu computador foi atualizado até 1 semana antes da data limite (29/11/2021)
- Abra Siate relatando a falta de atualização caso ocorra;

# Semana da Segurança da Informação – Ações

2. Verificar se o seu Windows está atualizado e na última versão;



- Como verificar a versão do seu Windows (Tabela de versões):

Canal Semestral						
Versão	Opção de manutenção	Data da disponibilidade	Data da última revisão	Latest OS build	Fim do serviço: Página Inicial, Pro, Pro Educação e Pro para Workstations	Fim do serviço: Enterprise, Education e IoT Enterprise
21H1	Canal Semestral	2021-05-18	2021-10-26	19043.1320	2022-12-13	2022-12-13
20H2	Canal Semestral	2020-10-20	2021-10-26	19042.1320	2022-05-10	2023-05-09
2004	Canal Semestral	2020-05-27	2021-10-26	19041.1320	2021-12-14	2021-12-14
1909	Canal Semestral	2019-11-12	2021-10-12	18363.1854	Fim do serviço	2022-05-10

# Semana da Segurança da Informação – Ações

2. Verificar se o seu Windows está atualizado e na última versão;



- Como verificar a versão do seu Windows (versões consideradas atualizadas):

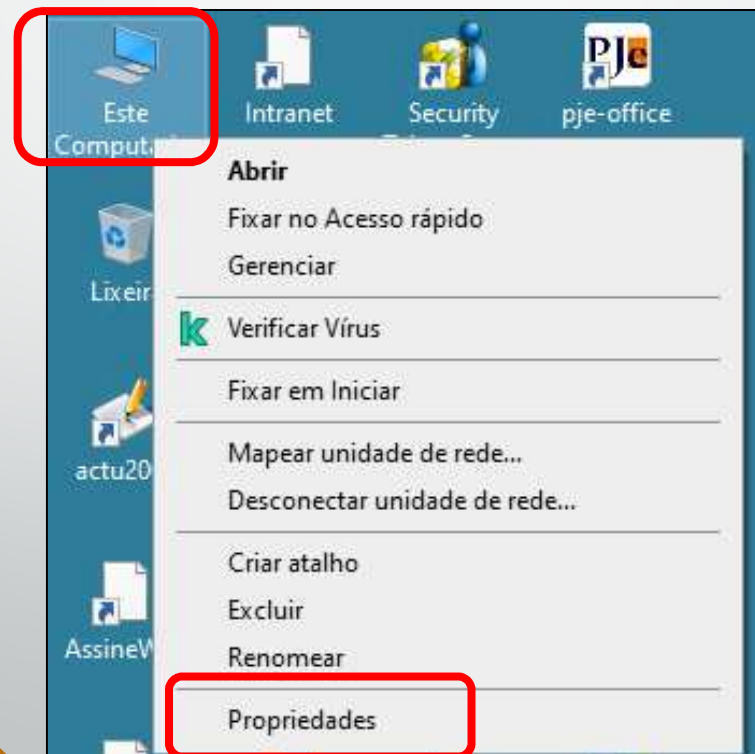
21H1	Canal Semestral
20H2	Canal Semestral
2004	Canal Semestral

# Semana da Segurança da Informação – Ações

2. Verificar se o seu Windows está atualizado e na última versão;



- Como verificar a versão do seu Windows:



# Semana da Segurança da Informação – Ações

2. Verificar se o seu Windows está atualizado e na última versão;



- Como verificar a versão do seu Windows:

The screenshot shows the Windows Settings application, specifically the 'Configurações' (Settings) window. The left sidebar lists various settings categories: Início, Sistema, Vídeo, Som, Notificações e ações, Assistente de foco, Energia e suspensão, and Bateria. The main content area is titled 'Sobre' (About) and displays system information. Under 'Especificações do Windows' (Windows specifications), the following details are shown:

Edição	Windows 10 Pro
Versão	21H1
Instalado em	01/09/2020
Compilação do SO	19043.1237
Experiência	Windows Feature Experience Pack 120.2212.3530.0

The 'Versão' (Version) field, showing '21H1', is highlighted with a red rectangular box. There are 'Copiar' (Copy) buttons for both the 'Sobre' section and the 'Especificações do Windows' section. A search bar is visible in the top left of the settings window with the placeholder text 'Localizar uma configuração'.



# Semana da Segurança da Informação – Ações

2. Verificar se o seu Windows está atualizado e na última versão;



- Como verificar a versão do seu Windows:

## Especificações do Windows

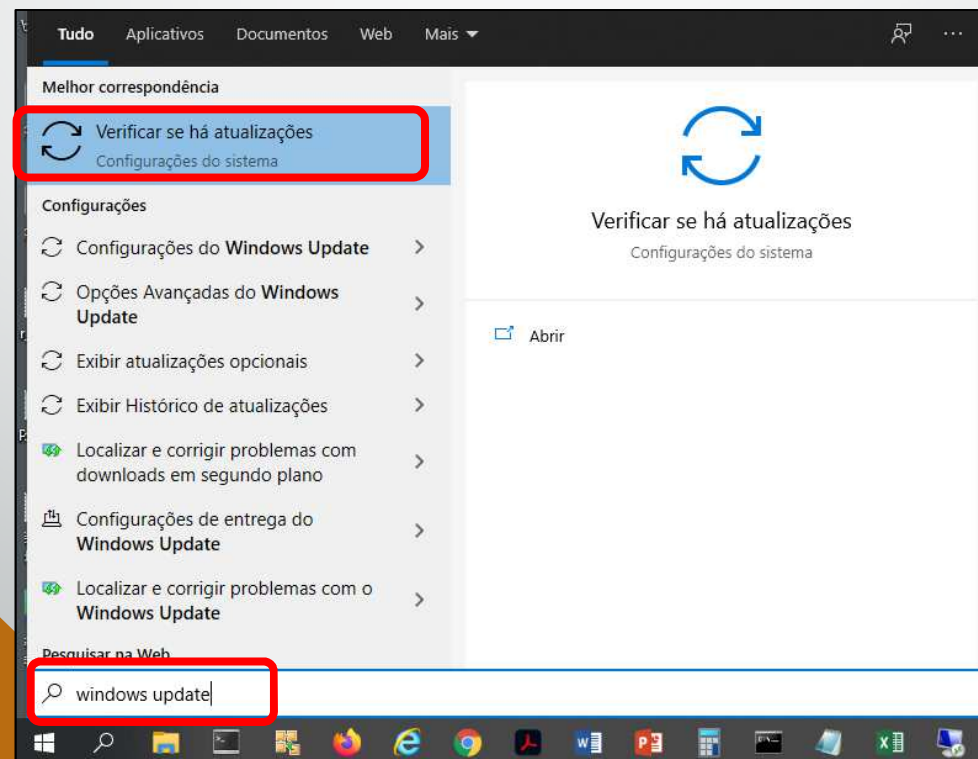
Edição	Windows 10 Pro
Versão	21H1
Instalado em	01/09/2020
Compilação do SO	19043.1237
Experiência	Windows Feature Experience Pack 120.2212.3530.0

# Semana da Segurança da Informação – Ações

2. Verificar se o seu Windows está atualizado e na última versão;



- Como verificar se Windows está atualizado:

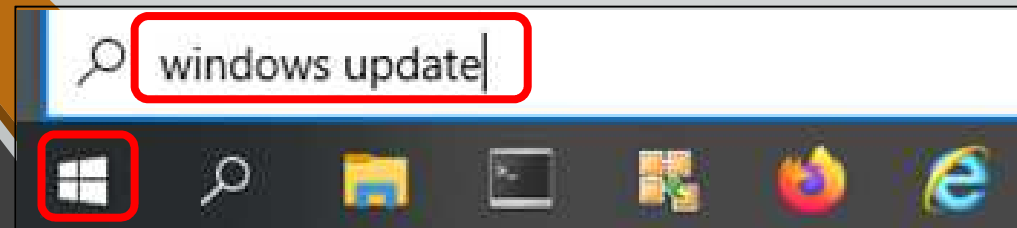
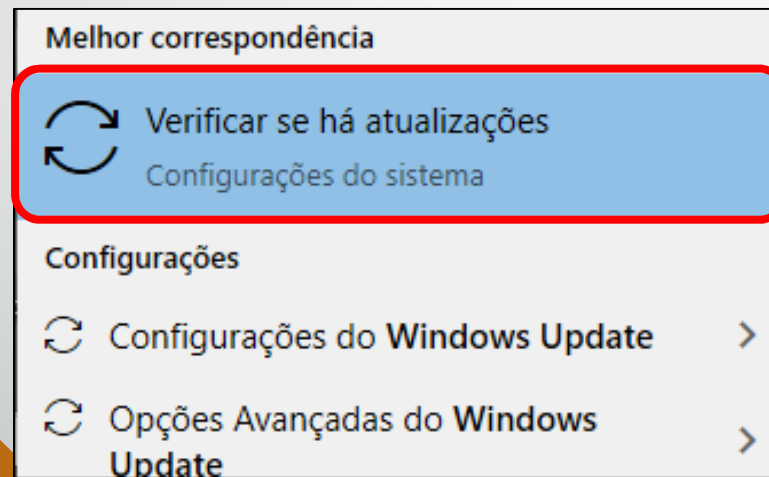


# Semana da Segurança da Informação – Ações

2. Verificar se o seu Windows está atualizado e na última versão;



- Como verificar se Windows está atualizado:



# Semana da Segurança da Informação – Ações

2. Verificar se o seu Windows está atualizado e na última versão;
  - Como verificar se Windows está atualizado:



## Windows Update

\*Algumas configurações são gerenciadas pela sua organização

[Exibir políticas de atualização configuradas](#)



Atualizações disponíveis

Última verificação: hoje, 08:25

Ferramenta de Remoção de Software Mal-intencionado do Windows x64 - v5.94 (KB890830)


**Status:** Instalação pendente

2021-10 Atualização Cumulativa do Windows 10 Version 21H1 para sistemas operacionais baseados em x64 (KB5006670)

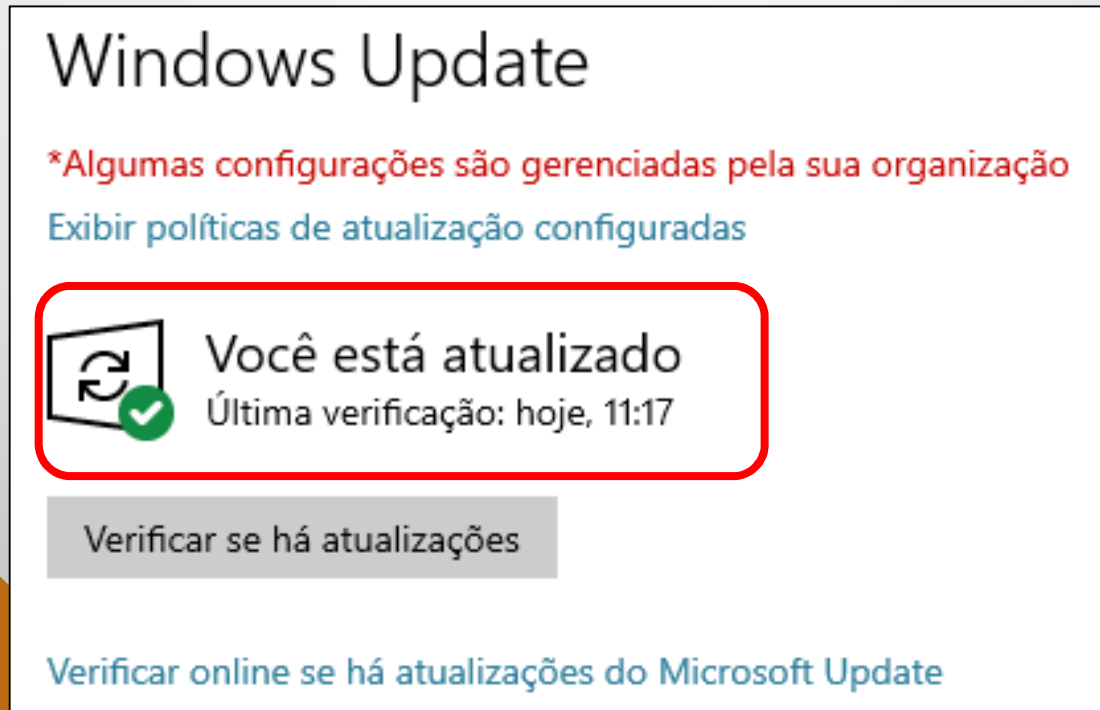
**Status:** Instalação pendente

Instalar agora

# Semana da Segurança da Informação – Ações

2. Verificar se o seu Windows está atualizado e na última versão;


  - Como verificar se Windows está atualizado:



Windows Update

\*Algumas configurações são gerenciadas pela sua organização

[Exibir políticas de atualização configuradas](#)

 **Você está atualizado**  
Última verificação: hoje, 11:17

[Verificar se há atualizações](#)

[Verificar online se há atualizações do Microsoft Update](#)

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet

- As senhas no TRT24 perdem a validade e são bloqueadas anualmente;
- Nos meses de abril/maio 2022 vencerá a data para troca de senhas de várias contas;
- Anote em sua agenda para não se esquecer de trocar;
- Na dúvida ou em algum evento estranho, sempre troque a senha;



# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet

- Como trocar a senha: acesse <https://intranet.trt24.jus.br>



**TRT24<sup>a</sup>**

**INTRANET**

Usuário :

Senha :

Acesso restrito a juizes e servidores do TRT da 24ª Região

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet

- Como trocar a senha: clique no ícone de alteração de senhas;



# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet


- Como trocar a senha: preencha os campos de alteração de senhas seguindo os critérios de força de senhas e clique no botão “Alterar Senha”

**Tribunal Regional do Trabalho**  
24ª Região | Mato Grosso do Sul

**Sigep - Intranet**

[Início](#) [Gabinetes e Circunscrições](#) [Secretarias e Diretorias](#) [Varas do Trabalho e Postos Avançados](#)

ALTERAÇÃO DE SENHA



Senha atual:

Nova Senha:

Redigite a Nova Senha:

**REGRAS de SEGURANÇA que devem ser seguidas para criação de sua Nova Senha:**

- 1º Ter No MÍNIMO 8 (oito) caracteres
- 2º Ter No MÁXIMO 20 (vinte) caracteres
- 3º Ter pelo menos UMA LETRA MAIÚSCULA
- 4º Ter pelo menos UMA LETRA MINÚSCULA
- 5º Ter pelo menos UM NÚMERO
- 6º Ter pelo menos UM DOS SEGUINTE CARACTERES ESPECIAIS: @ ! # \$ % &
- 7º **NÃO** pode ter três números repetidos em sequência; por exemplo: 333 111
- 8º **NÃO** pode ter três números em sequência; por exemplo: 012 567 789

\* **Você deve criar uma NOVA SENHA, e esta não pode ser igual à sua senha ATUAL.**

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas

### 1. Não trocar a senha até o vencimento:

- Caso possua e-mail de recuperação cadastrado: Acessar a Intranet <https://intranet.trt24.jus.br> e preencher o campo “Usuário” com seu login e clicar no link “clique aqui caso tenha esquecido sua senha” na página inicial da Intranet.



**Tribunal Regional do Trabalho**  
24ª Região | Mato Grosso do Sul

**INTRANET**

Usuário : fmsilva

Senha :

Entrar Limpar Sair

Acesso restrito a juizes e servidores do TRT da 24ª Região

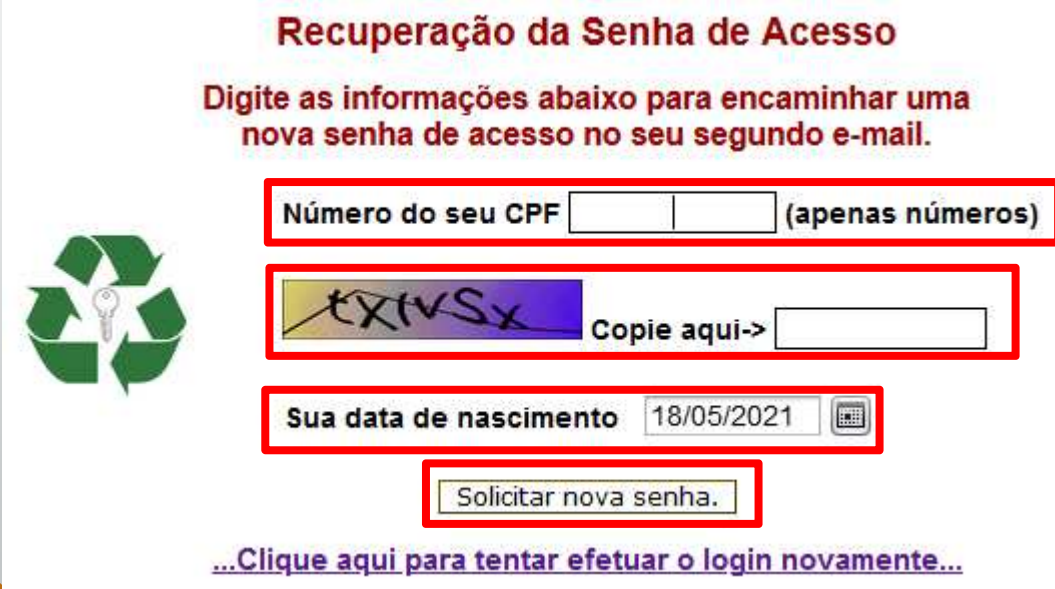
[Clique aqui caso tenha esquecido sua senha.](#)

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas


### 1. Não trocar a senha até o vencimento:

- Caso possua e-mail de recuperação cadastrado: na janela que aparecer, preencher o campo CPF, Captcha, data de nascimento e clicar no botão “Solicitar nova senha”.





**Recuperação da Senha de Acesso**

Digite as informações abaixo para encaminhar uma nova senha de acesso no seu segundo e-mail.



Número do seu CPF   (apenas números)

 Copie aqui->

Sua data de nascimento  

[...Clique aqui para tentar efetuar o login novamente...](#)



# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas


### 1. Não trocar a senha até o vencimento:

- Caso possua e-mail de recuperação cadastrado: Mensagem de “senha encaminhada para (email@pessoal) com sucesso” será mostrada.

**Recuperação da Senha de Acesso**

**Digite as informações abaixo para encaminhar uma nova senha de acesso no seu segundo e-mail.**

Número do seu CPF  (apenas números)

  Copie aqui->

Sua data de nascimento  

**Senha encaminhada para (fabio.\*\*\*\*\*@gmail\*\*\*\*\*) com sucesso!  
Verifique na caixa de Entrada ou caixa de Spam a sua nova senha.**

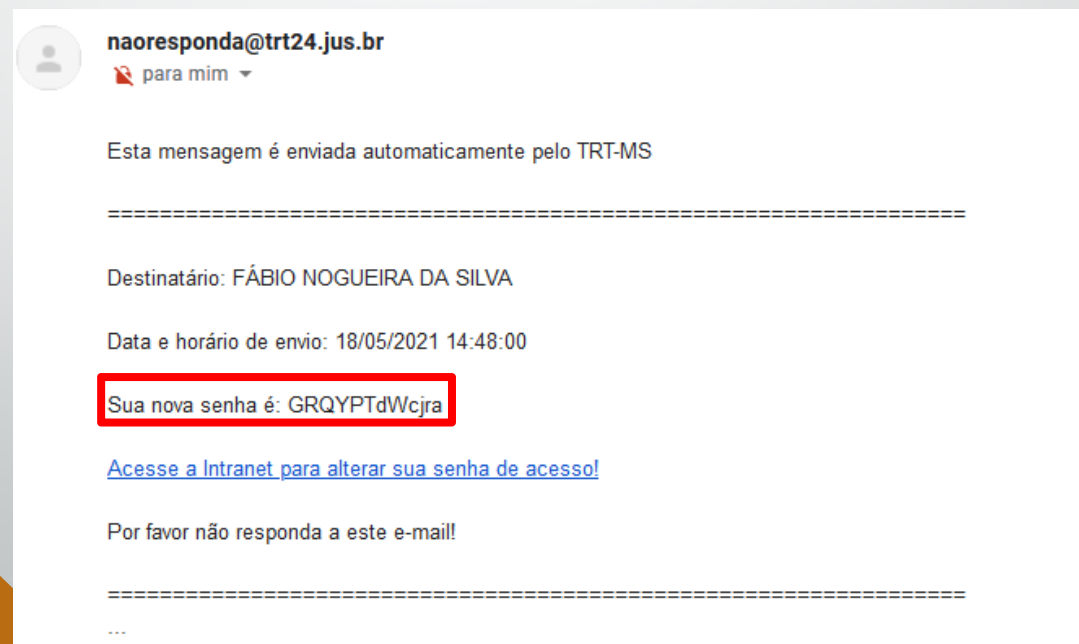
[...Clique aqui para tentar efetuar o login novamente...](#)

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas

### 1. Não trocar a senha até o vencimento:

- Caso possua e-mail de recuperação cadastrado: verificar caixa de entrada de email de recuperação, trocar a senha na intranet utilizando como senha atual a senha informada nesse email.





# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas

### 1. Não trocar a senha até o vencimento:

- Se não possuir e-mail de recuperação cadastrado :
  - Peça ao seu chefe imediato que abra um SIATE, informando o celular seguro para que você possa ser contatado. Ligar diretamente para a central de serviços não é recomendável por conta do ataque de engenharia social.
  - Apresente-se ao CGP – Coordenadoria de Gestão de Pessoas – para cadastrar o seu e-mail de recuperação assim que possível. No próximo recadastramento anual, essa informação será obrigatória.

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas

### 1. Não trocar a senha até o vencimento:

- Se não possuir e-mail de recuperação cadastrado: **é possível se cadastrar no SIGEP-Online**. Para isso:
- Entre na nossa intranet em <https://intranet.trt24.jus.br>

**Tribunal Regional do Trabalho**  
24ª Região | Mato Grosso do Sul

**INTRANET**

Usuário : fnsilva

Senha :

Entrar Limpar Sair

Acesso restrito a juizes e servidores do TRT da 24ª Região

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas

### 1. Não trocar a senha até o vencimento:

- Se não possuir e-mail de recuperação cadastrado: **é possível se cadastrar no SIGEP-Online.** Para isso:
- Clique na opção “Sistemas” do menu principal

The screenshot shows the Intranet interface for the Tribunal Regional do Trabalho 24ª Região. The header includes the logo and name of the court, the user name 'Sr. FÁBIO NOGUEIRA', and the department 'SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO'. The main navigation menu is located at the top, with the 'Sistemas' option highlighted by a red box. Below the menu, a grid of system icons is displayed under the heading 'SISTEMAS'. The systems listed include AssineWeb, Aud4, Avaliação de Servidores, Certidão Online, Detran-MS, EAD da Escola Judicial, eConsig Consignados, e-DOC viewer, FUNPRESP-JUD, Gabinete Virtual, Gabinete Virtual Novo, GEST - Gestão de Estagiários, Gestore Web, Inscrições Cursos Escola Judicial, Junta Comercial, Malote Digital, PJe - 1º Grau, PJe - 2º Grau, PJe-Calc Cálculo Trabalhista, PJEDoc Sentença Eletrônica, Processo Adm. PROAD, Projeção Aposentadoria, SCMP - Material e Patrimônio, SIATE - Abrir chamado, SIGEP-Online, SIG Gerenciamento, SIGS - Sistema Integrado de Gestão em Saúde, Sistema de Recadastramento, Site TRT24, and WebMail Institucional.

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas

### 1. Não trocar a senha até o vencimento:

- Se não possuir e-mail de recuperação cadastrado: **é possível se cadastrar no SIGEP-Online**. Para isso:
- Na tela que aparecer, clique no sistema SIGEP-Online

The screenshot displays the Intranet interface of the Tribunal Regional do Trabalho 24ª Região | Mato Grosso do Sul. The header includes the logo and name of the tribunal, the user name 'Sr. FÁBIO NOGUEIRA', and the role 'SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMU'. Below the header is a navigation menu with options: 'Início', 'Gabinetes e Circunscrições', 'Secretarias e Diretorias', 'Varas do Trabalho e Postos Avançados', 'Serviços e Informações', and 'Sistemas'. The main content area is titled 'SISTEMAS' and contains a grid of buttons for various systems. The 'SIGEP-Online' button is highlighted with a red border. Other systems listed include AssineWeb, Aud4, Avaliação de Servidores, Certidão Online, Detran-MS, EAD da Escola Judicial, eConsign Consignados, e-DOC viewer, FUNPRESP-JUD, Gabinete Virtual, Gabinete Virtual Novo, GEST - Gestão de Estagiários, Gestore Web, Inscrições Cursos Escola Judicial, Junta Comercial, Malote Digital, PJe - 1º Grau, PJe - 2º Grau, PJe-Calc Cálculo Trabalhista, PJEDoc Sentença Eletrônica, Processo Adm. PROAD, Projeção Aposentadoria, SCMP - Material e Patrimônio, SIATE - Abrir chamado, SIG Gerenciamento, SIGS - Sistema Integrado de Gestão em Saúde, Sistema de Recadastramento, Site TRT24, and WebMail Institucional.

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas

### 1. Não trocar a senha até o vencimento:

- Se não possuir e-mail de recuperação cadastrado: **é possível se cadastrar no SIGEP-Online**. Para isso:
- Você será direcionado à tela inicial do SIGEP-Online. Basta se logar nessa tela com seu usuário e senha.

JUSTIÇA DO TRABALHO SIGEP-Online  
Sistema Integrado de Gestão de Pessoas - Módulo Online

Login - Autenticação de usuário Resolução CSJT 217 versão: 21.5.0.1 - atualização: 13/05/2021 15:04:17

Autenticação de Usuário

Usuário:

Senha:

Entrar

Por favor, digite sua matrícula.



# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas

### 1. Não trocar a senha até o vencimento:

- Se não possuir e-mail de recuperação cadastrado: **é possível se cadastrar no SIGEP-Online**. Para isso:
  - Depois de entrar no sistema, vá em “Serviços ao Magistrado/Servidor” – “Alteração de Dados Pessoais”



The screenshot displays the SIGEP-Online interface for the Justiça do Trabalho. The header includes the logo and the text "SIGEP-Online Sistema Integrado de Gestão de Pessoas - Módulo Online". The main navigation bar contains links for "Consultas", "Serviços ao Magistrado/Servidor", "Alteração de senha", and "Sair". A dropdown menu is open under "Serviços ao Magistrado/Servidor", with "Alteração de Dados Pessoais" highlighted. Other menu items include "Espelho de Ponto", "Ajuda Judiciária ao Juiz Substituto", "Alteração de Dados Bancários", "Declaração de IRPF", "Férias", "Avaliação de Desempenho", and "TRTeiros". The page also contains informational text and a footer with contact information.

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – possíveis problemas

### 1. Não trocar a senha até o vencimento

- Se não possuir e-mail de recuperação cadastrado: **é possível se cadastrar no SIGEP-Online**. Para isso:
- Na tela de “Alteração de Dados Pessoais”, preencha o campo “E-mail externo” com seu email de recuperação. Clicar no botão “Confirmar” para salvar as alterações.

Alteração de Dados Pessoais versão: 21.5.0.1 - atualização: 13/05/2021 15:04:17

Dados Pessoais	
Nascimento:	Sexo:
Naturalidade:	Nacionalidade:
Estado Civil:	Escolaridade:
Tipo sanguíneo:	Doador de Órgãos:
País:	Cidade:
U.F.:	Complemento:
Endereço:	CEP:
Número:	Celular:
Bairro:	Cartão Nacional de Saúde: <input checked="" type="radio"/> Não possui <input type="radio"/> Possui
Fone:	
E-mail Externo:	
Nome do Pai:	
Conjuge/Companheiro(a):	



# Semana da Segurança da Informação – Ações

3. Mudar sua senha na Intranet – possíveis problemas
2. Máquinas FORA da rede do TRT24 – teletrabalho ordinário
  - A senha para login no Windows NÃO será atualizada por falta de comunicação do sistema com o Domínio de Autenticação.
  - Solução: utilizar a senha antiga apenas para entrar no Windows. Levar o computador ao TRT24 assim que possível para sincronização de senha.
  - Nova senha funcionará normalmente nos demais sistemas do TRT24.

# Semana da Segurança da Informação – Ações

## 3. Mudar sua senha na Intranet – dicas

- **JAMAIS** anote sua senha **em papel**;
- **JAMAIS** salve as senhas em **texto plano**;
- Para ajudar nessa tarefa, temos a lista de alguns programas gerenciadores de senhas:
  - LastPass: <https://www.lastpass.com/pt>
  - Keepass: <https://keepass.info/>
  - Kaspersky: <https://www.kaspersky.com.br/password-manager>
- Para facilitar a tarefa de NÃO anotar senhas, a SETIC realizará testes em diversas ferramentas e incluirá a escolhida em sua imagem padrão do Windows em breve;

# Fontes

- [1] Pesquisa PWC 2018 - <https://www.pwc.com.br/pt/global-state-of-information-security-survey-2018/colaboradores-atuais-continuam-a-ser-a-principal-fonte-de-incidentes-de-seguranca.html>
- [2] <https://g1.globo.com/politica/noticia/2021/05/07/supremo-investiga-tentativa-de-ataque-hacker-a-sistema-da-corte.ghtml>
- [3] <https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/05/06/nove-dias-apos-ataque-cibernetico-tj-rs-ainda-enfrenta-dificuldades-para-acessar-processos.ghtml>

## Fontes

- [4] <https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataque-de-hackers-ao-sistema-do-tribunal.ghtml>
- [5] <https://g1.globo.com/sao-paulo/noticia/sites-do-governo-de-sp-do-tj-e-do-mp-saem-do-ar-apos-ciberataques-em-larga-escala.ghtml>
- [6] <https://g1.globo.com/sp/vale-do-paraiba-regiao/noticia/2020/12/01/embraer-e-alvo-de-ataque-cibernetico-e-investiga-impactos.ghtml>
- [7] <https://g1.globo.com/economia/tecnologia/noticia/2021/05/10/o-ataque-de-hackers-a-maior-oleoduto-dos-eua-que-fez-governo-declarar-estado-de-emergencia.ghtml>

# Fontes

- [8] <https://g1.globo.com/economia/tecnologia/noticia/2021/02/24/ataques-hacker-a-hospitais-e-farmaceuticas-aumentam-com-a-pandemia-aponta-ibm.ghtml>
- [9] <https://www.campograndenews.com.br/cidades/capital/hackers-que-alteravam-processos-federais-sao-alvo-de-operacao-da-pf>
- [10] <https://www.antivirusguide.com/pt/melhor-antivirus/>