JUSTIÇA DO TRABALHO
80 anos
Tribunal Regional do Trabalho da 24ª Região (MS)

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.

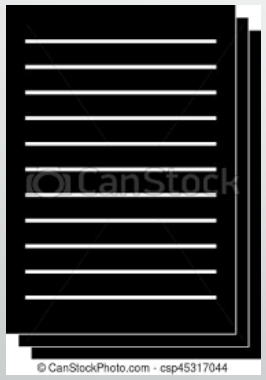
O que é a informação?

- 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.

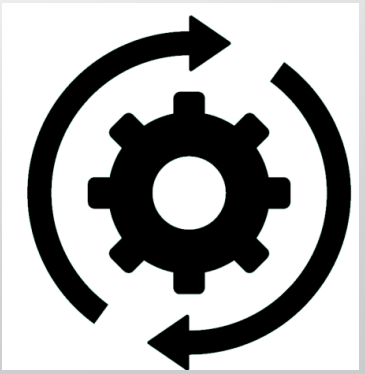
Distribuição da informação

Pessoas

Equipamentos de TI



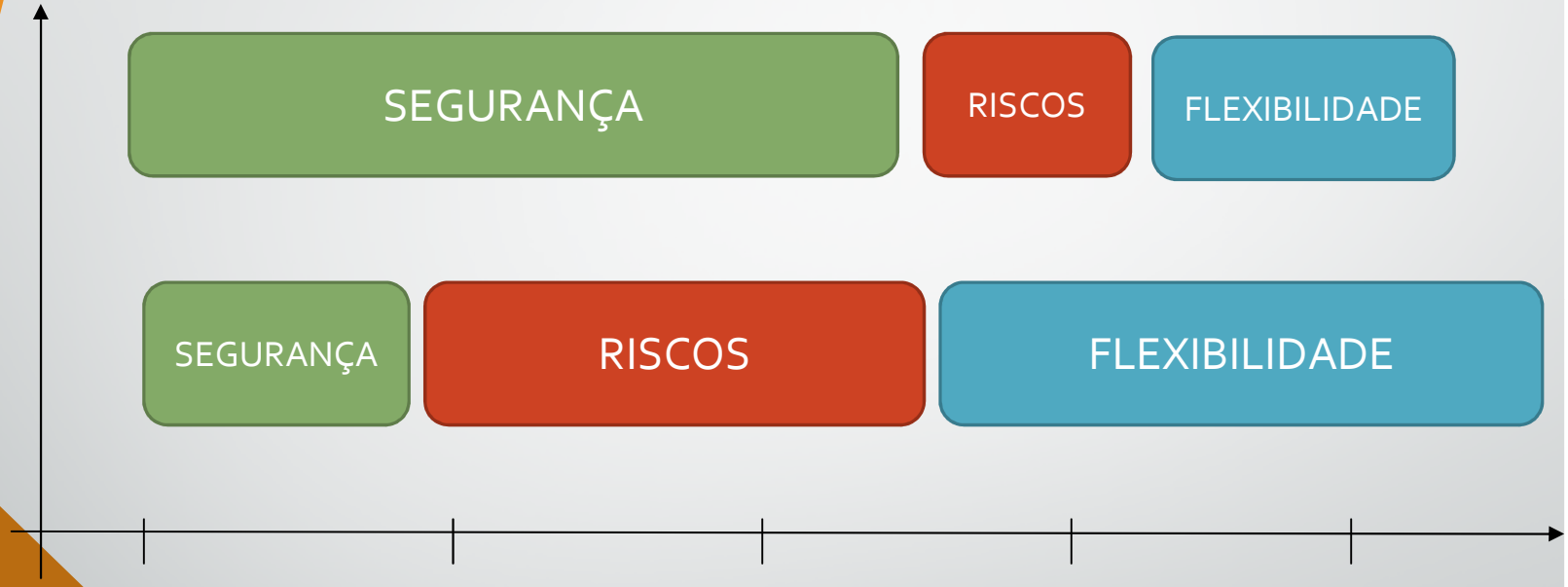
Papéis e documentos



Sistemas e processos de trabalho

Precisamos proteger a informação

Desafios para proteção da informação

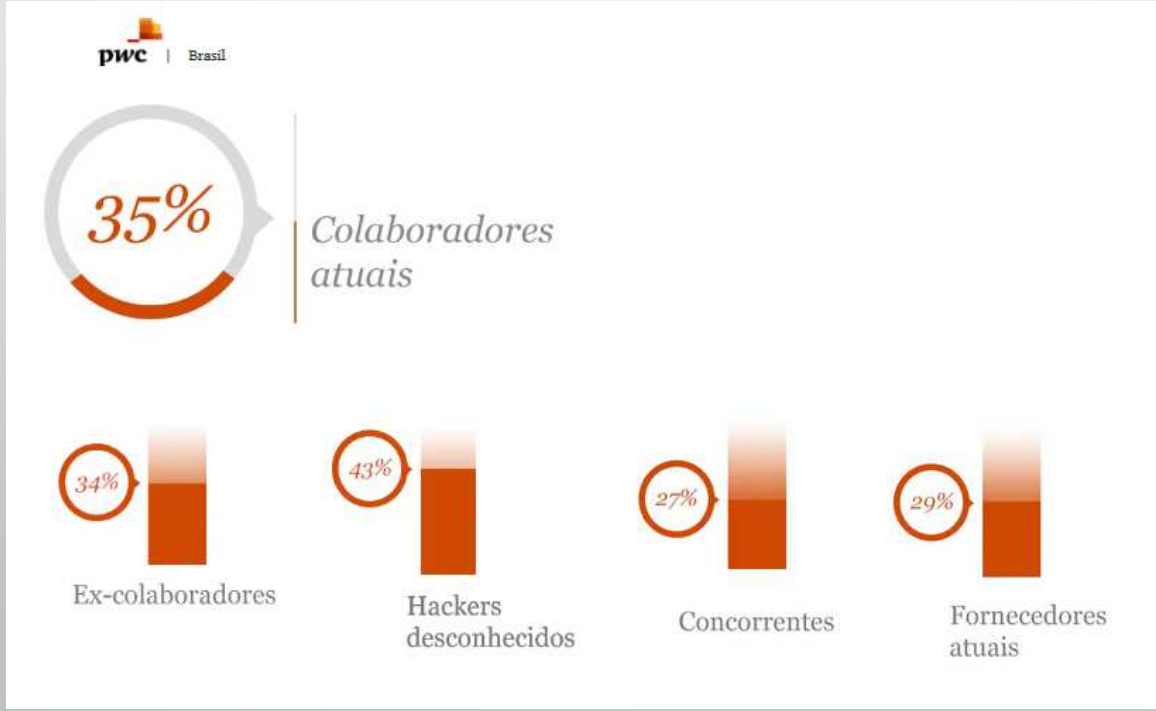


Níveis de Segurança, Risco e Flexibilidade

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
  - TRT4 - ransoware
  - TJ/SP - ransoware
  - STJ - ransoware
  - STF – Sql Injection

Por que você é tão importante ?

- Notícias recentes de ataques cibernéticos

06/05/2021

07/05/2021

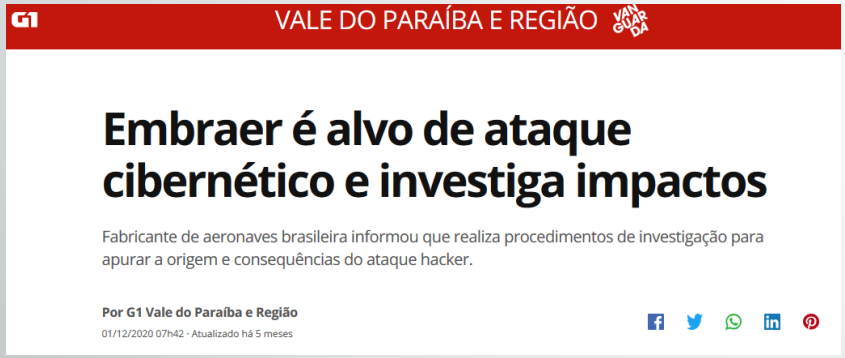
04/11/2020

12/05/2017

Por que você é tão importante ?

- Notícias recentes de ataques cibernéticos

01/12/2020


G1 VALE DO PARAÍBA E REGIÃO VANGUARDA

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

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

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

19/05/2021


Menu NEWS
Capital

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 que você é tão importante ?

- Notícias recentes de ataques cibernéticos

30/09/2021

JUSTIÇA DO TRABALHO
TRT da 4ª Região (RS)

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.

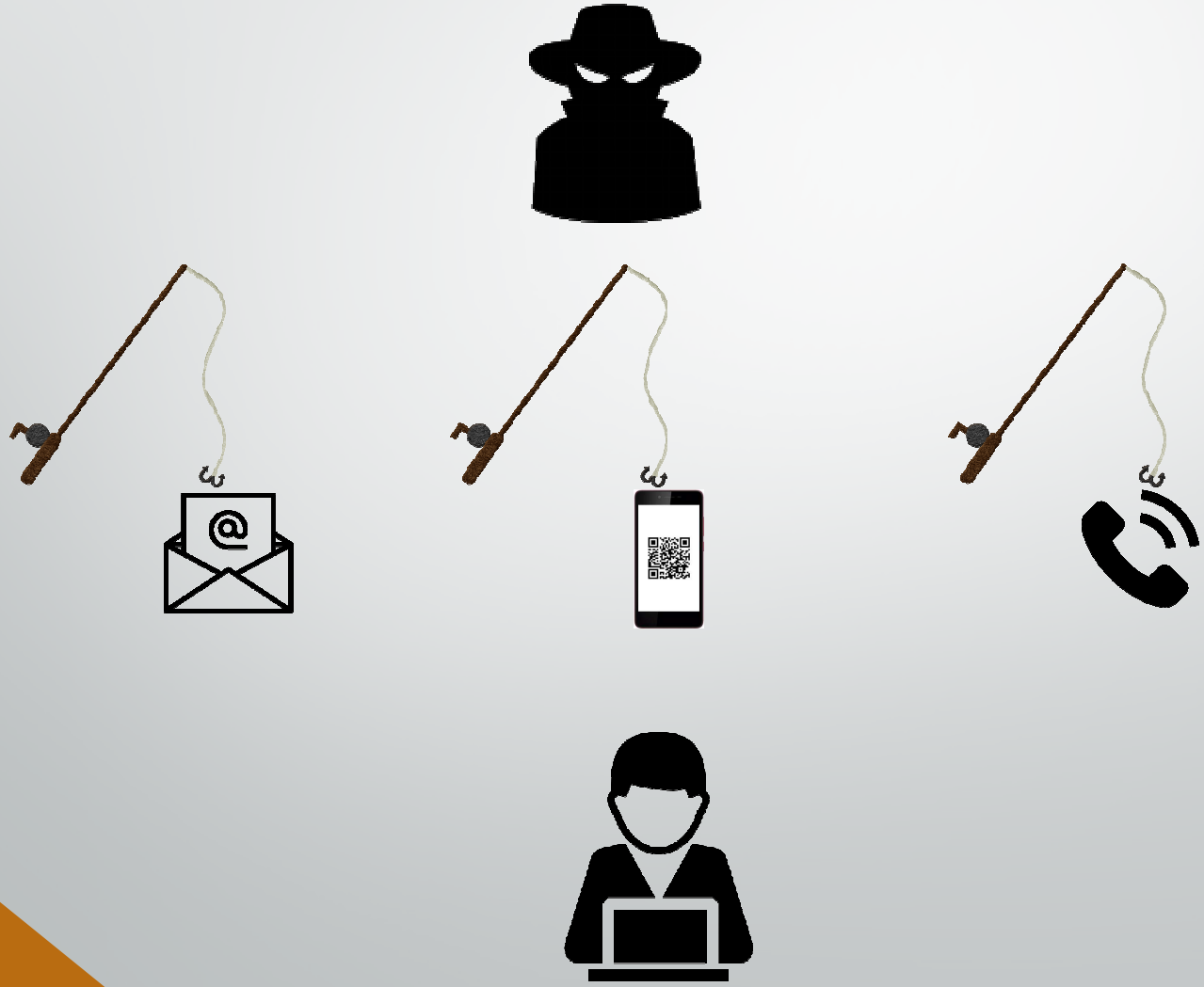
Imediatamente após a confirmação do ataque cibernético, a equipe técnica da Secretaria de Tecnologia da Informação e Comunicações do TRT4 (SETIC) executou as medidas de isolamento e contenção dos danos potenciais, a fim de preservar a segurança e a integridade das informações.

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.

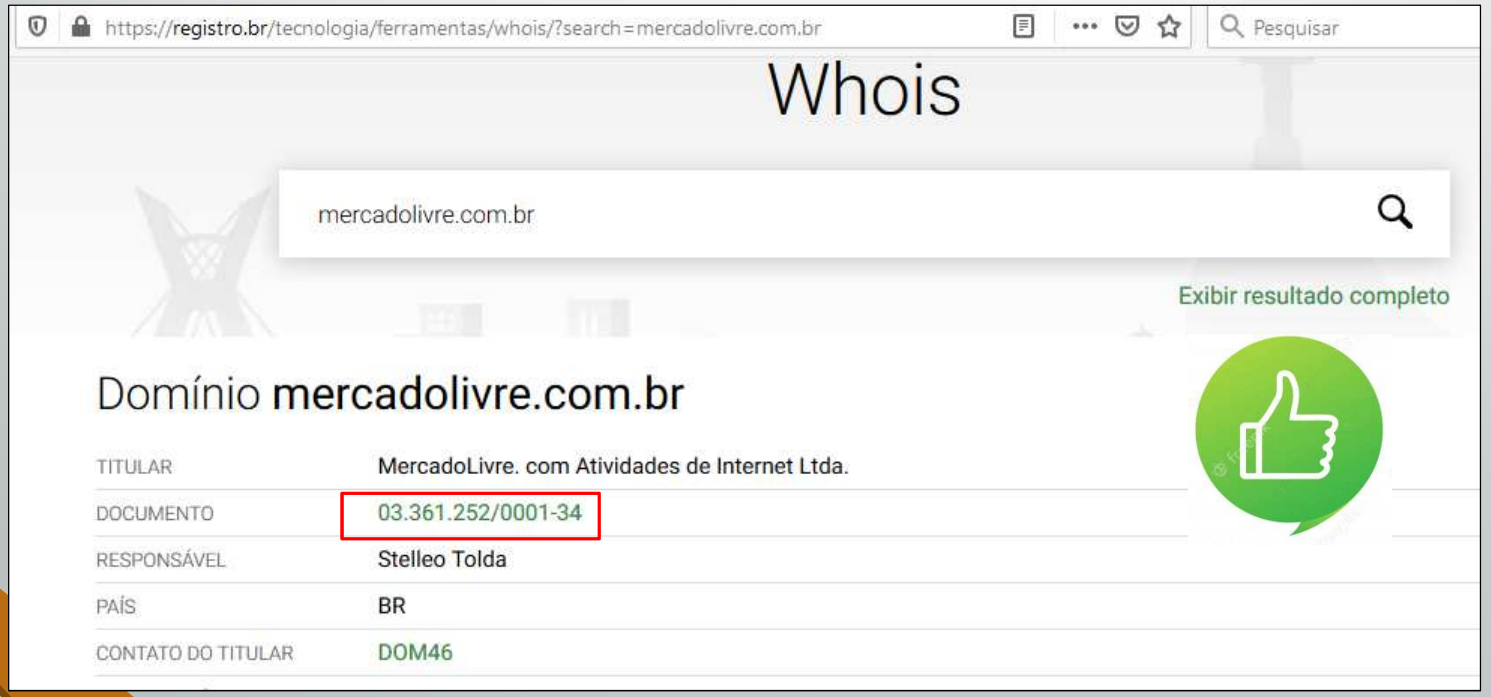


- Engenharia social
  1. Phishing: Tentativa de induzir o usuário a clicar em uma URL **parecida** com a verdadeira.

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

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

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



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

- 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,

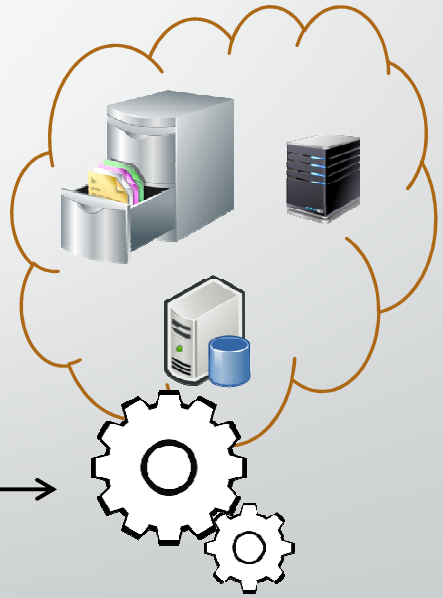
Equipe do MercadoLivre.

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

Equipamentos TRT24



Parte da aplicação Pje rodando no navegador do seu computador

Parte da aplicação Pje rodando nos equipamentos do TRT24

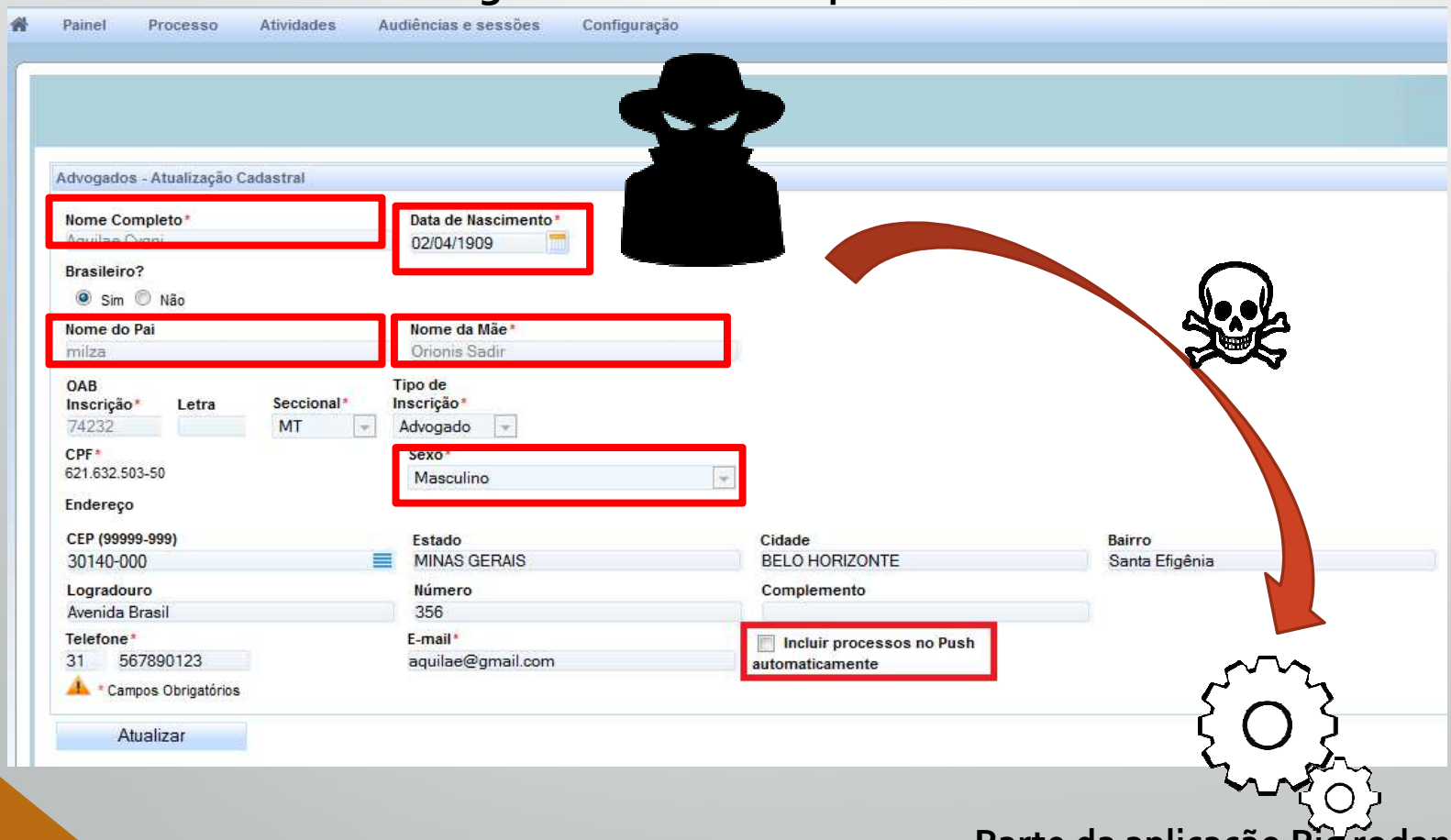
- Engenharia social
  2. XSS, injeções e "DNS Poisoning": Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso
     - XSS – Cross Site Scripting e pontos de injeção

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



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>
Data: 28 de outubro de 2021 13:43:12 AMT
Para: <fabio.nogueira86@gmai.com>
Assunto: Altere o PIN do seu token para não perder o acesso ao PJe

80 anos JUSTIÇA DO TRABALHO
Tribunal Regional do Trabalho da 24ª Região (MS)

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>
Data: 28 de outubro de 2021 13:43:12 AMT
Para: <fabio.nogueira86@gmai.com>
Assunto: Altere o PIN do seu token para não perder o acesso ao PJe

JUSTIÇA DO TRABALHO
Tribunal Regional do Trabalho da 24ª Região (MS)

Prezado usuário,

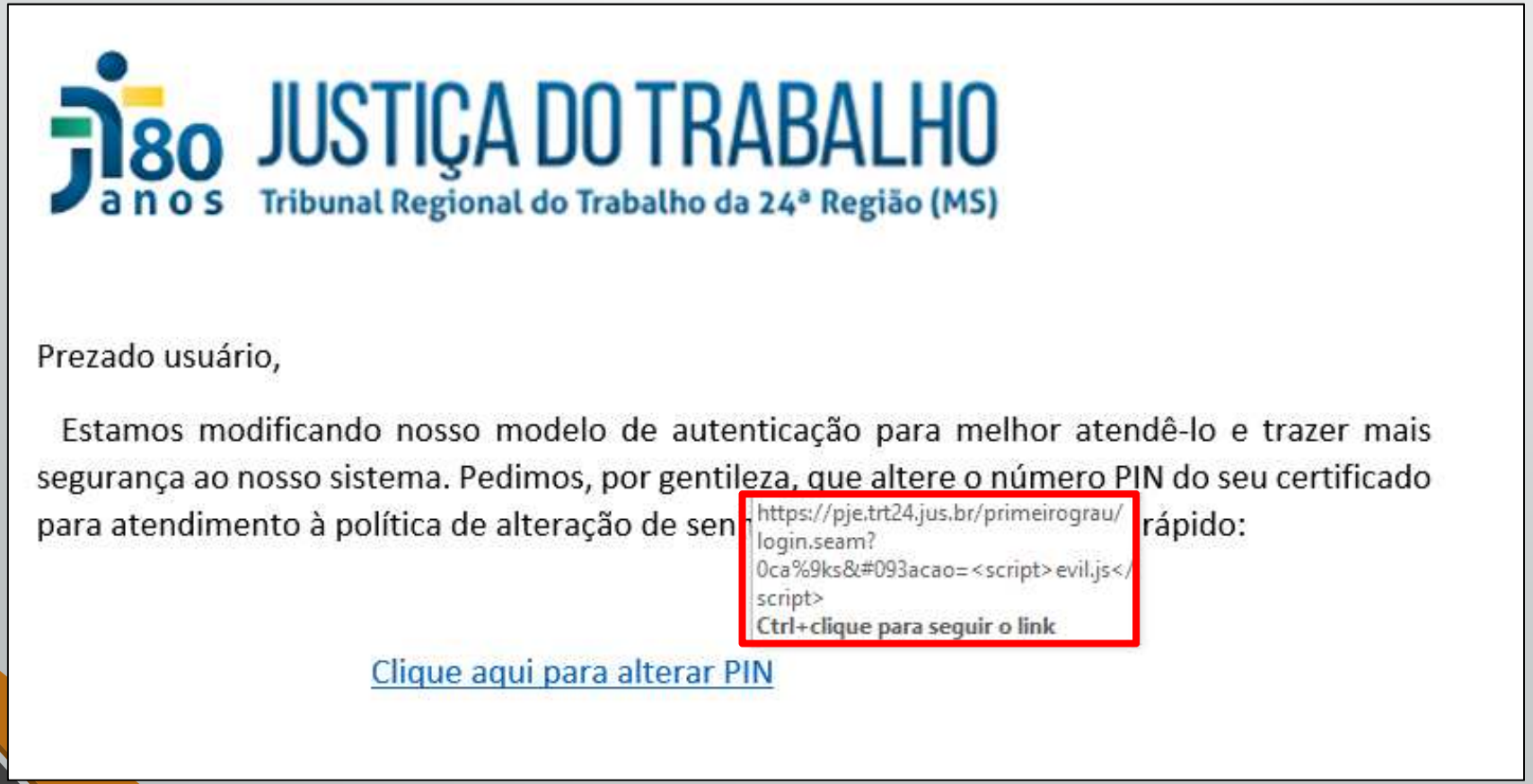
Estamos modificando nosso modelo de autenticação para melhor atendê-lo e trazer mais segurança ao nosso sistema. Pedimos, por gentileza, que altere o número PIN do seu certificado para atendimento à política de alteração de senhas. Segue link para acesso rápido:

Clique aqui para alterar PIN

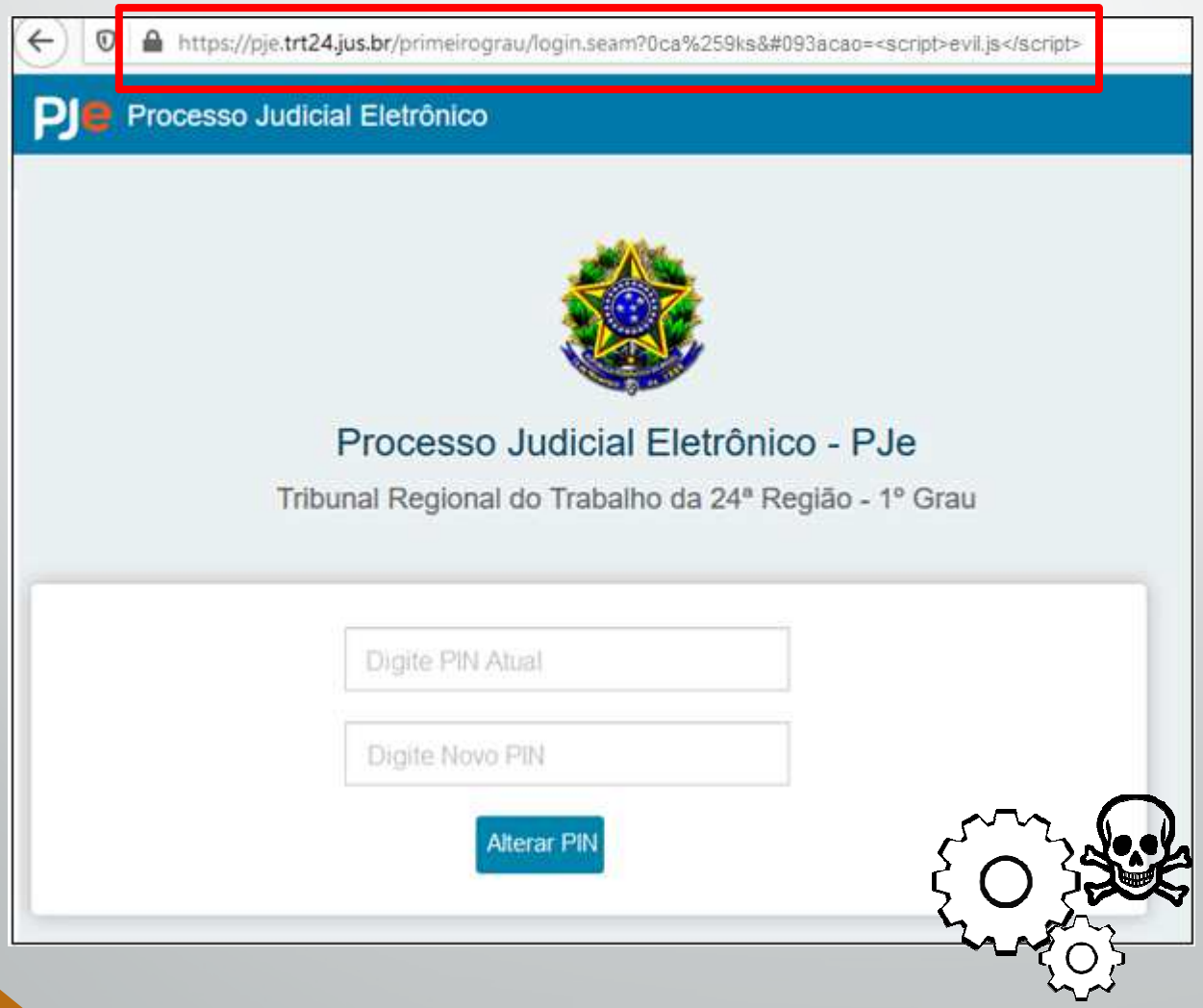
Atenciosamente:
Equipe de TI do TRT24

- 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



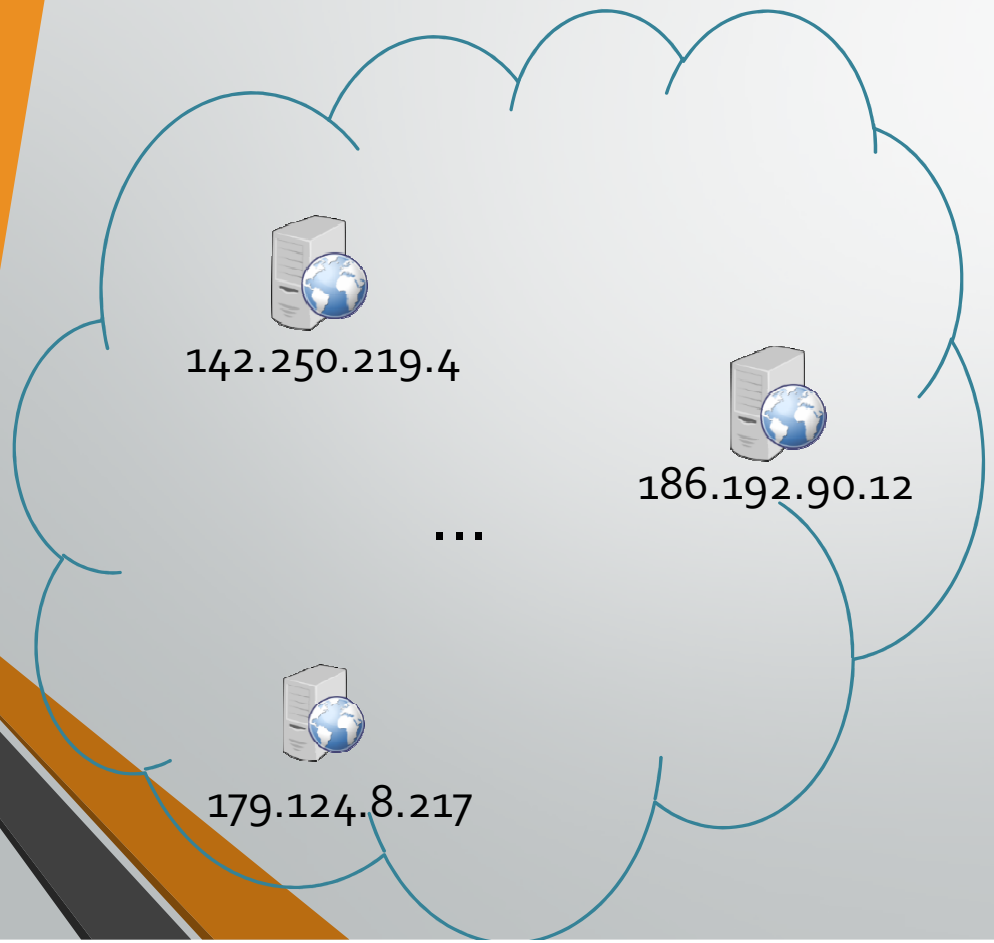
- Engenharia social
  2. XSS, injeções e "DNS Poisoning": Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira injetando código malicioso
     - XSS – Cross Site Scripting e pontos de injeção;



- 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

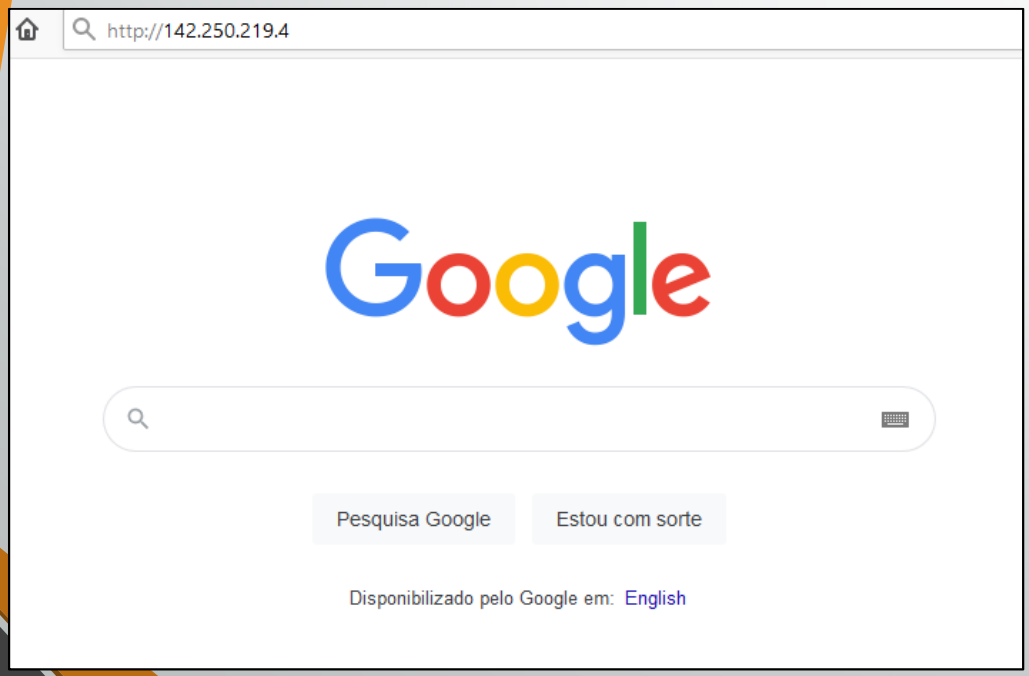
142.250.219.4 -> google.com

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

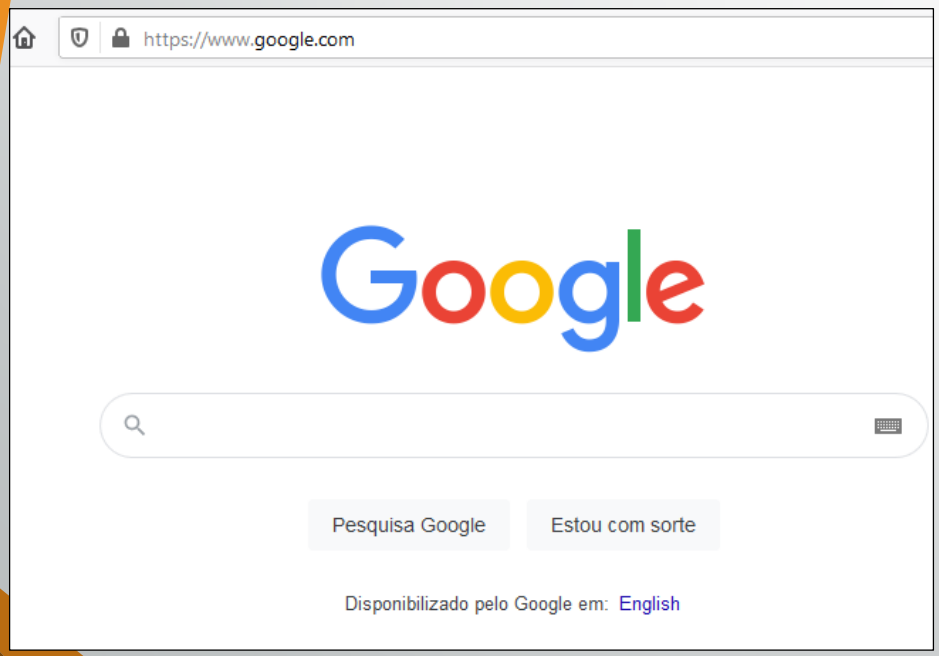
186.192.90.12 -> globo.com

...

- 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

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

...

- 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

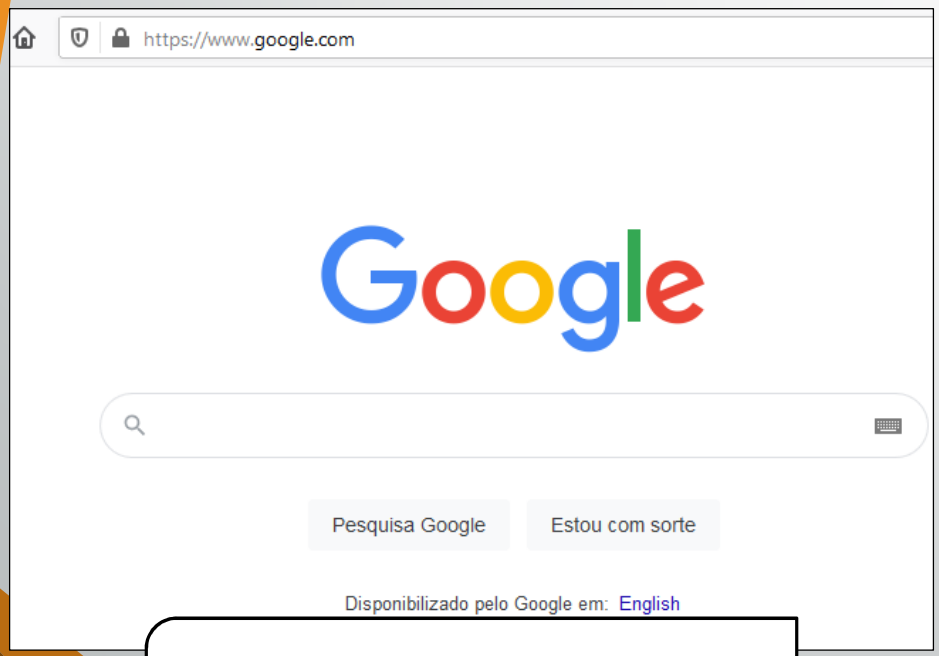
Servidor DNS

142.250.219.4 -> google.com

179.124.8.217 -> pje.trt24.jus.br

186.192.90.12 -> globo.com

...

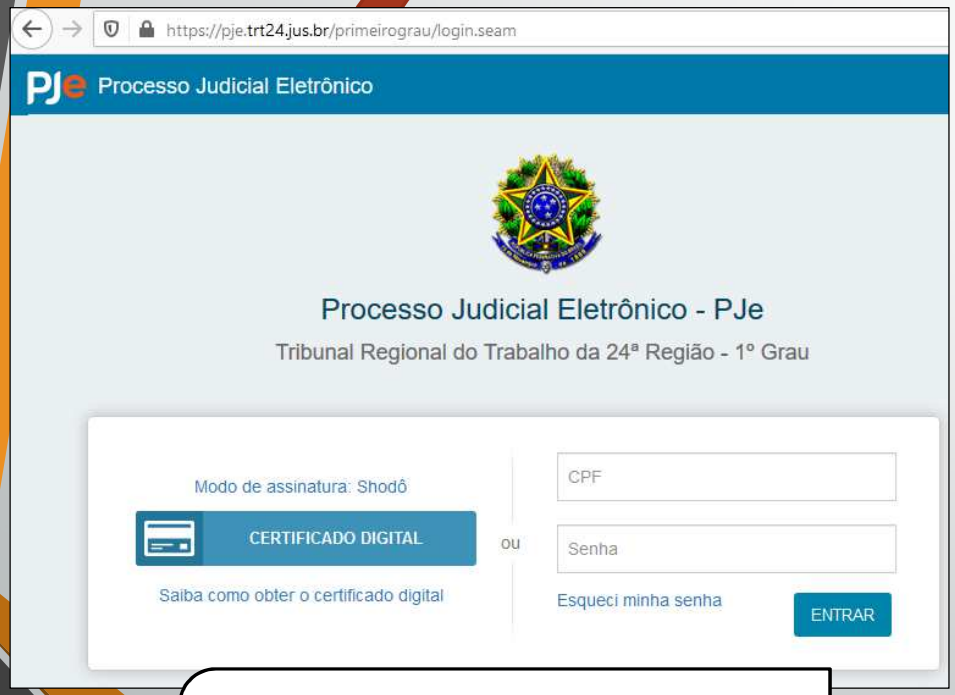


Cache DNS local do computador
142.250.219.4 ->google.com

- 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

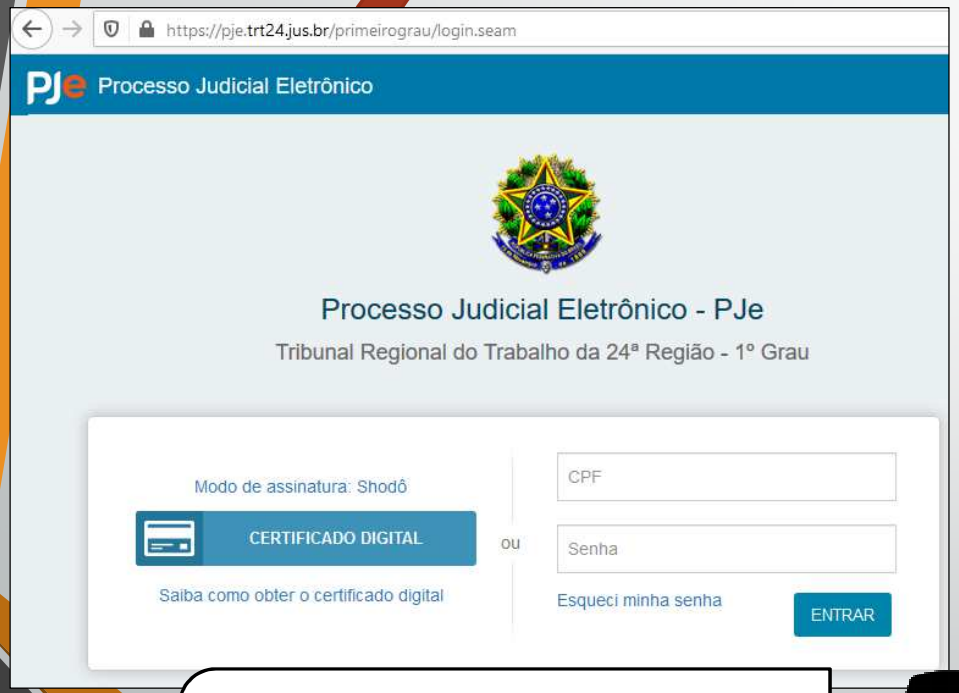
Servidor DNS

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>
Data: 28 de outubro de 2021 13:43:12 AMT
Para: <fabio.nogueira86@gmai.com>
Assunto: Altere o PIN do seu token para não perder o acesso ao PJe

80 anos JUSTIÇA DO TRABALHO
Tribunal Regional do Trabalho da 24ª Região (MS)

Prezado usuário,

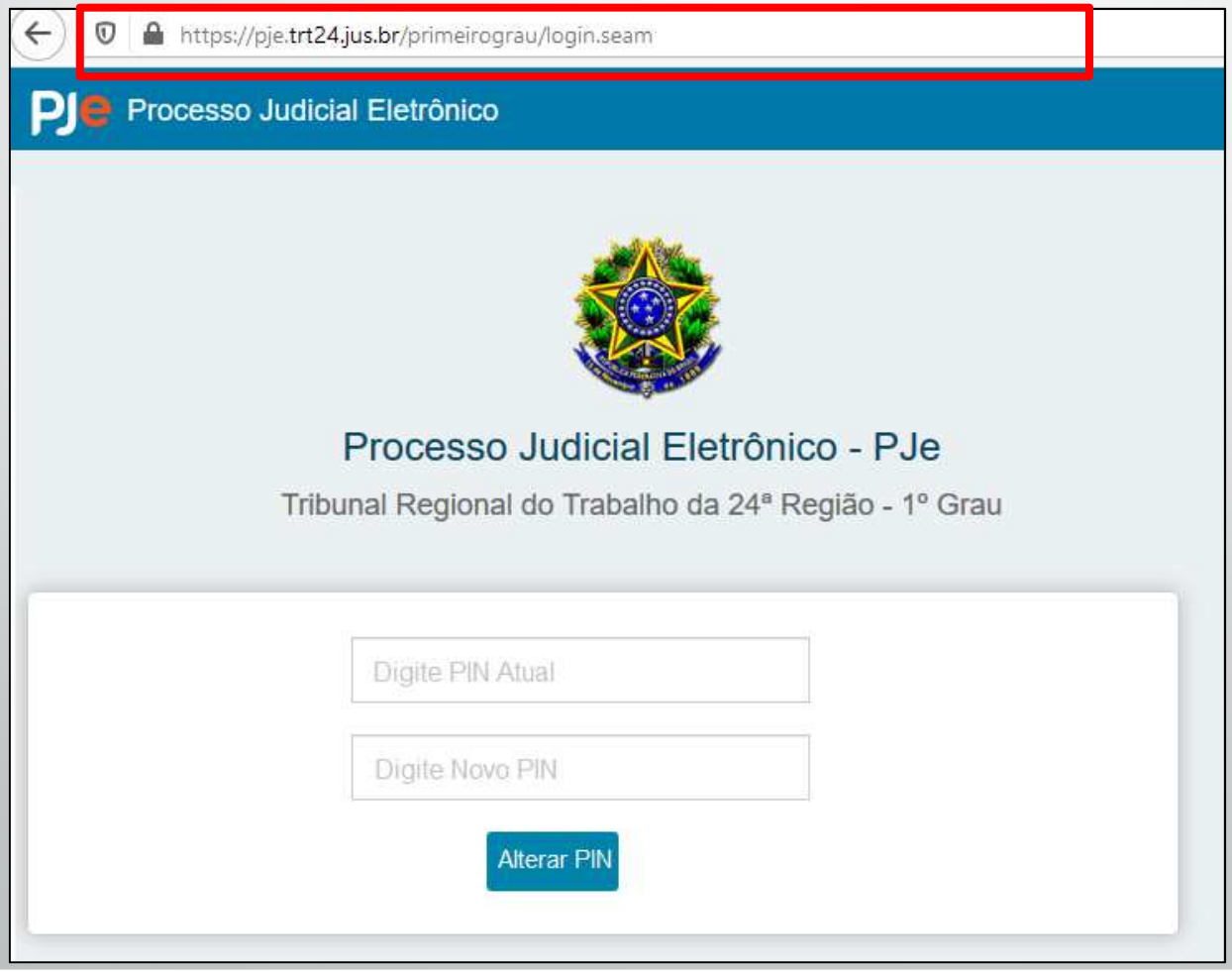
Estamos modificando nosso modelo de autenticação para melhor atendê-lo e trazer mais segurança ao nosso sistema. Pedimos, por gentileza, que altere o número PIN do seu certificado para atendimento à política de alteração de senhas. Segue link para acesso rápido:

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

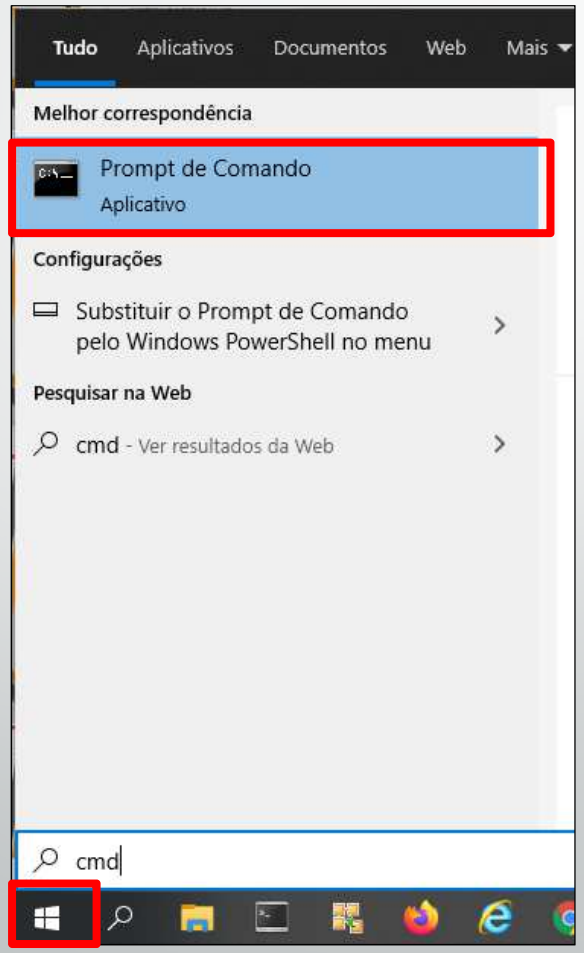
Atenciosamente:
Equipe de TI do TRT24

- 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

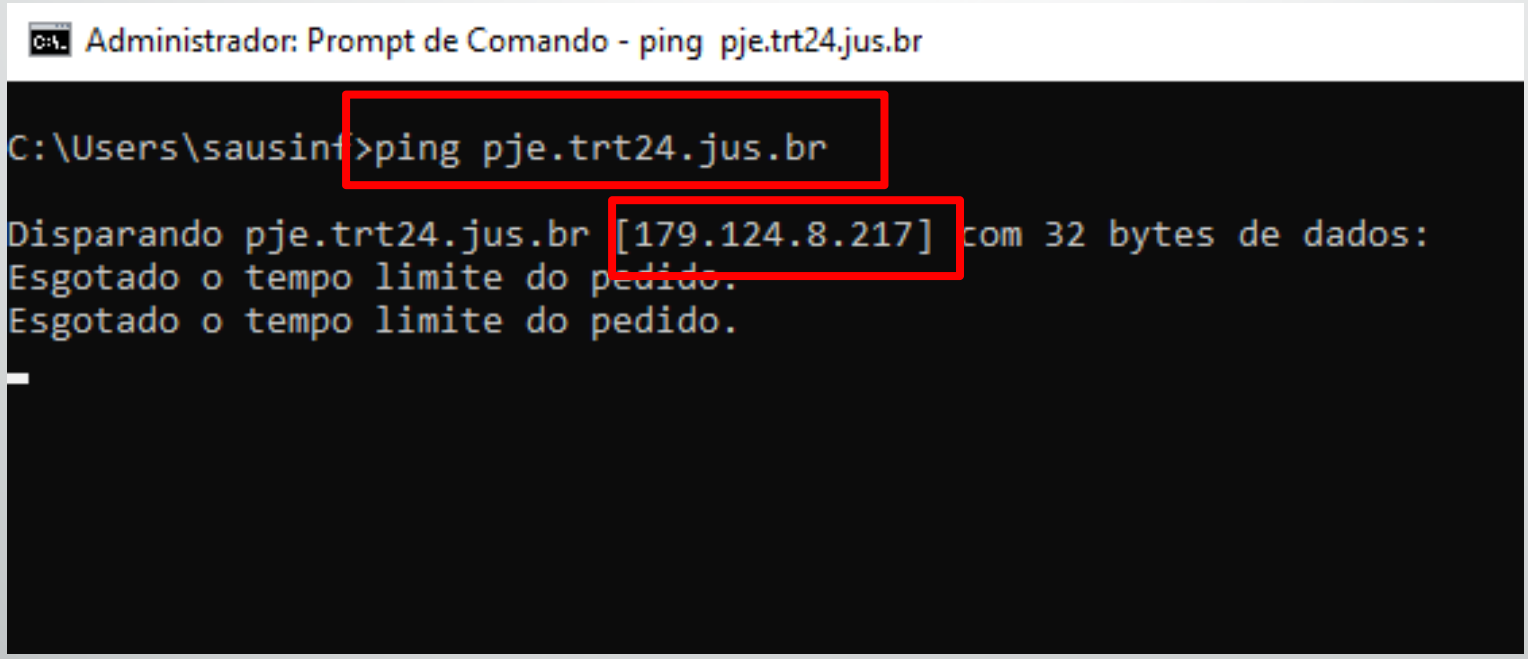
DNS Poisoning para finalizar o ataque



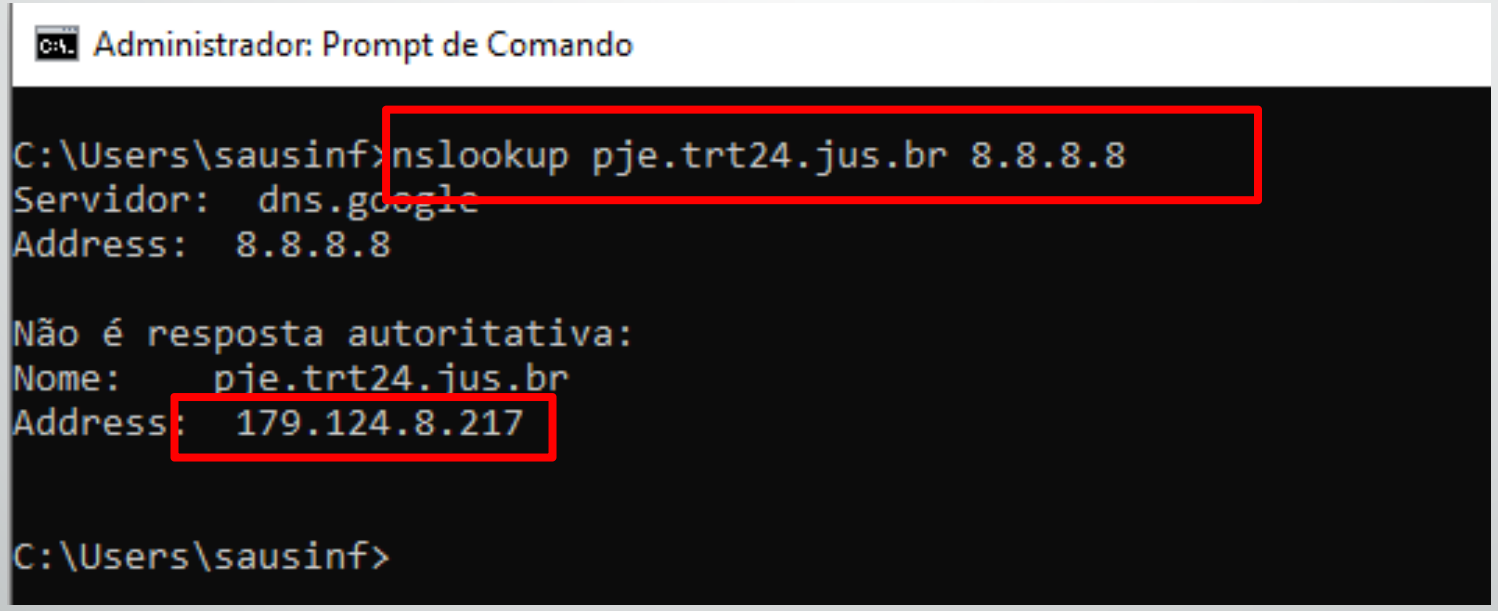
- Engenharia social
  2. XSS, injeções e "DNS Poisoning": Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;
     - DNS Poisoning – envenenamento de DNS: como verificar se estou contaminado ?



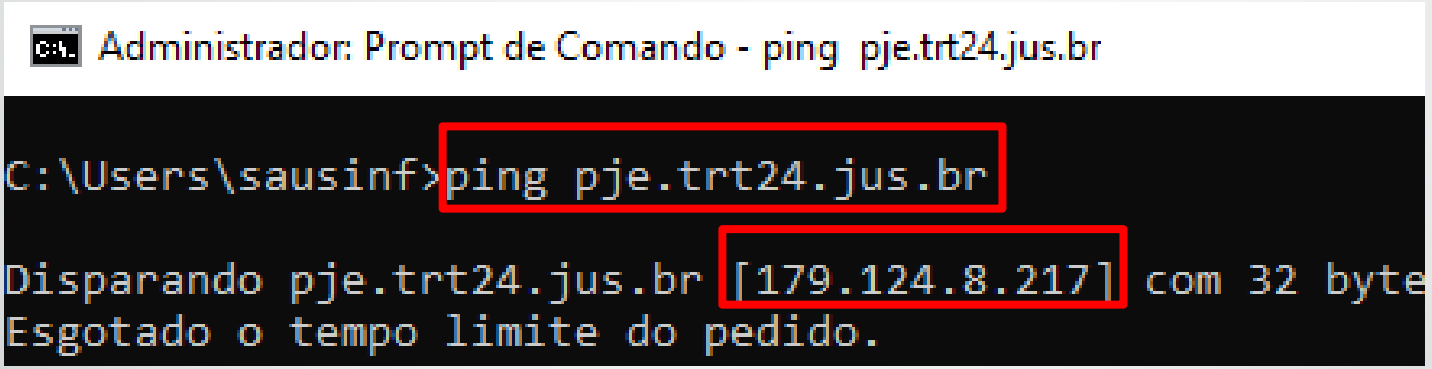
- Engenharia social
  2. XSS, injeções e "DNS Poisoning": Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;
     - DNS Poisoning – envenenamento de DNS: como verificar se estou contaminado ?

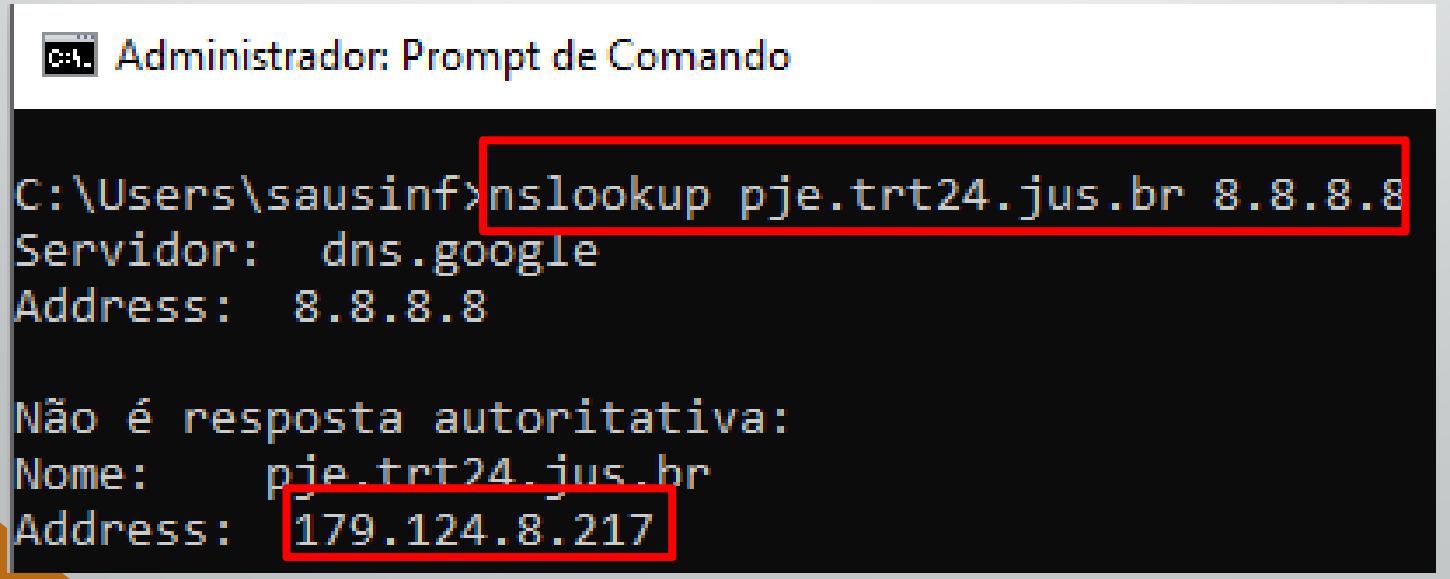


- Engenharia social
  2. XSS, injeções e "DNS Poisoning": Tentativa de induzir o usuário a clicar em uma URL **igual** a verdadeira envenenando cache DNS;
     - DNS Poisoning – envenenamento de DNS: como verificar se estou contaminado ?
       - **8.8.8.8** é o endereço IP do DNS do google, de conhecimento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



- 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 ?





- # Contramedidas

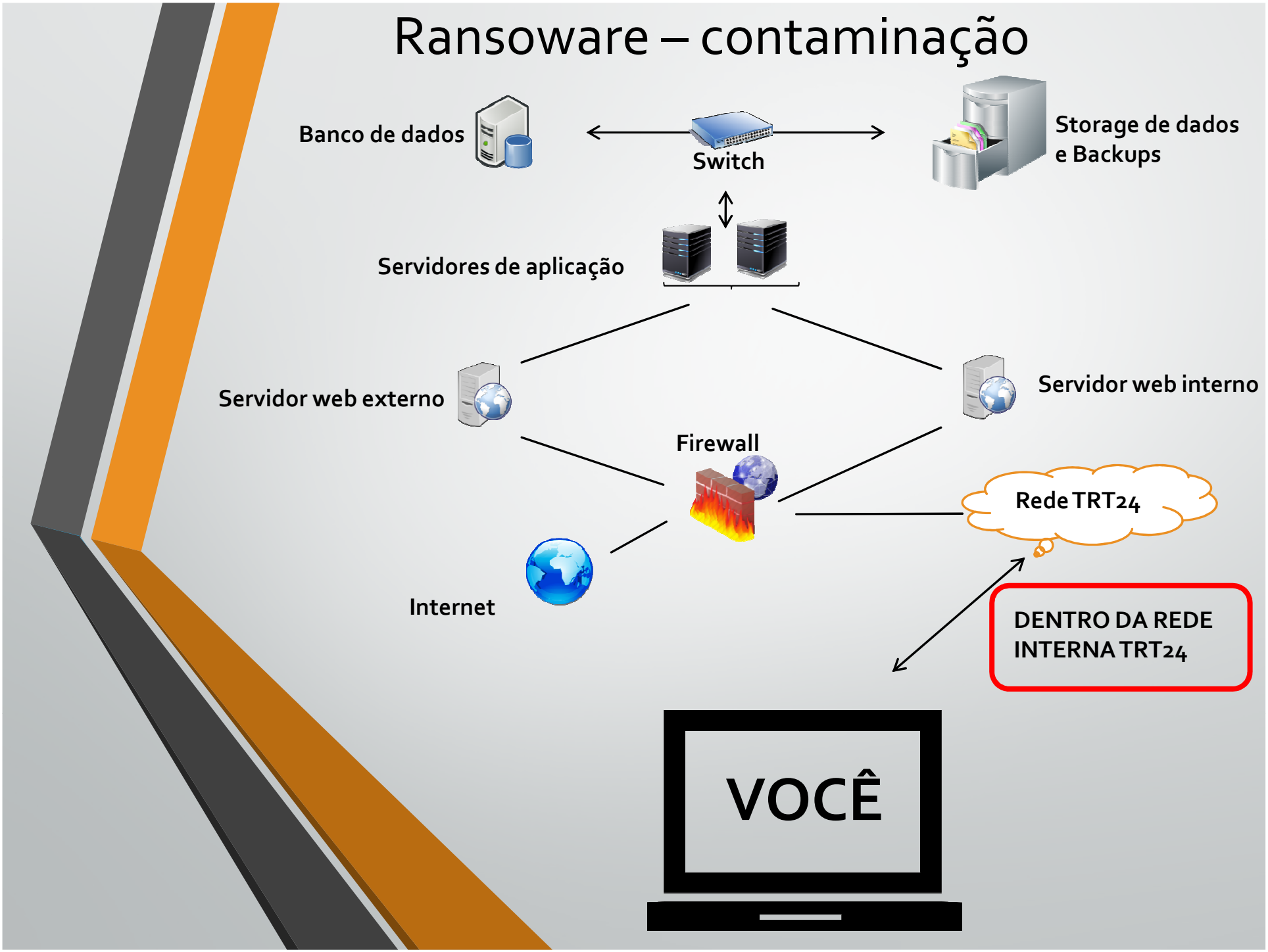
1. Phishing;
2. XSS, injeções e “DNS Poisoning”

- ✓ 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 relacionado ao trabalho;

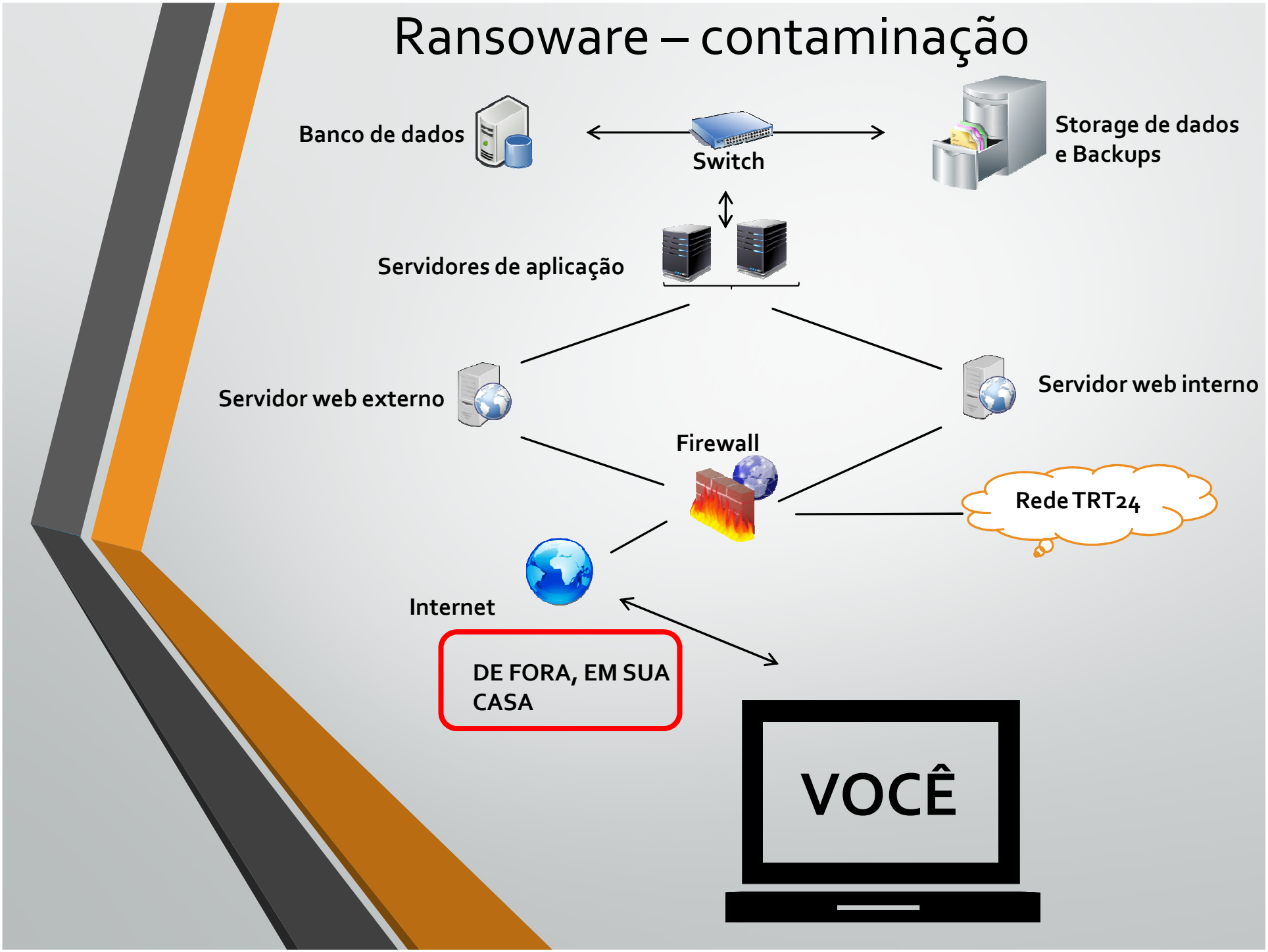
Principais ataques à Segurança da Informação e contramedidas

- Engenharia social
  3. Ransoware – Sequestro de informação;

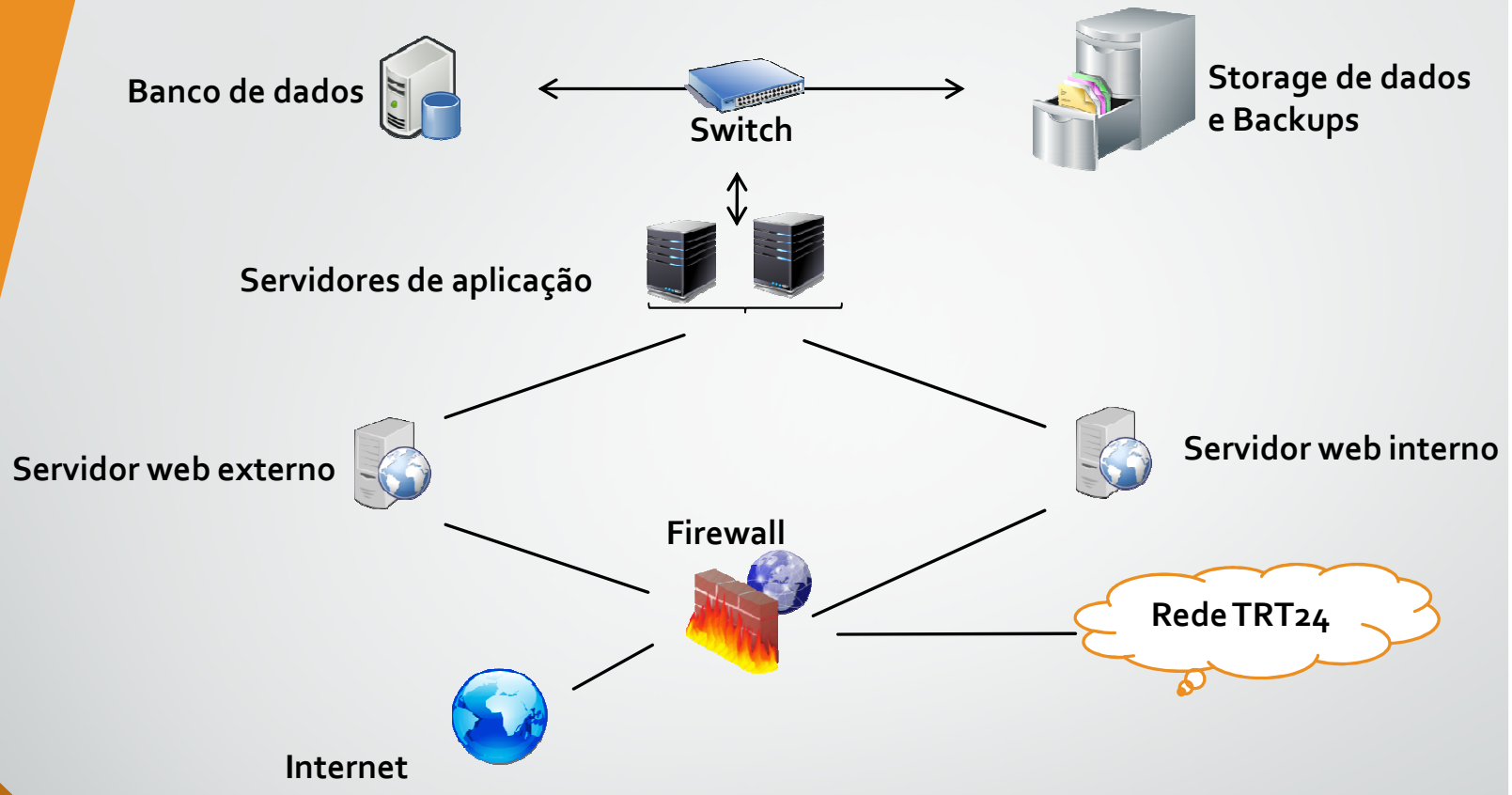
Ransoware – contaminação



Ransoware – contaminação

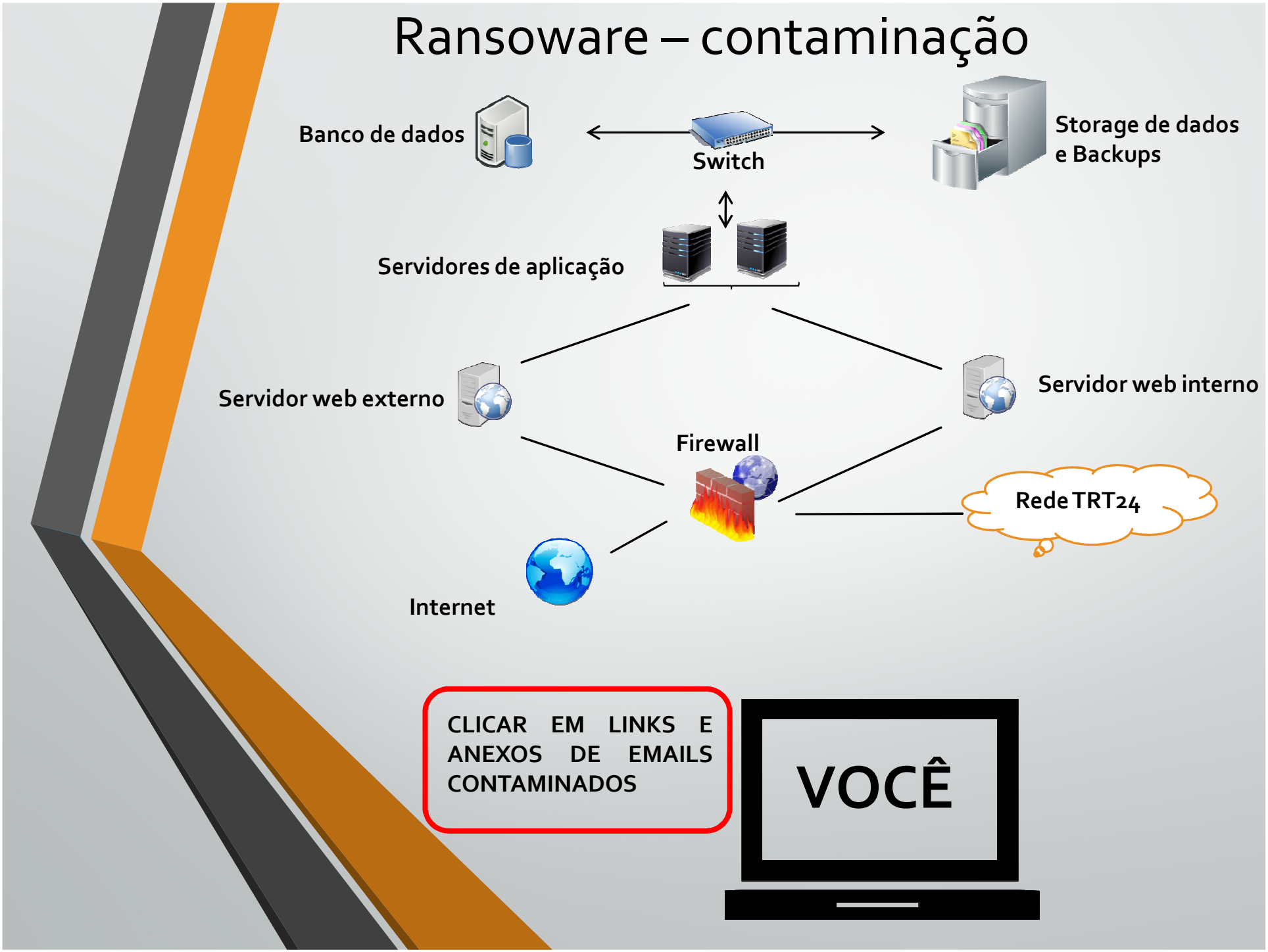


Ransoware – contaminação

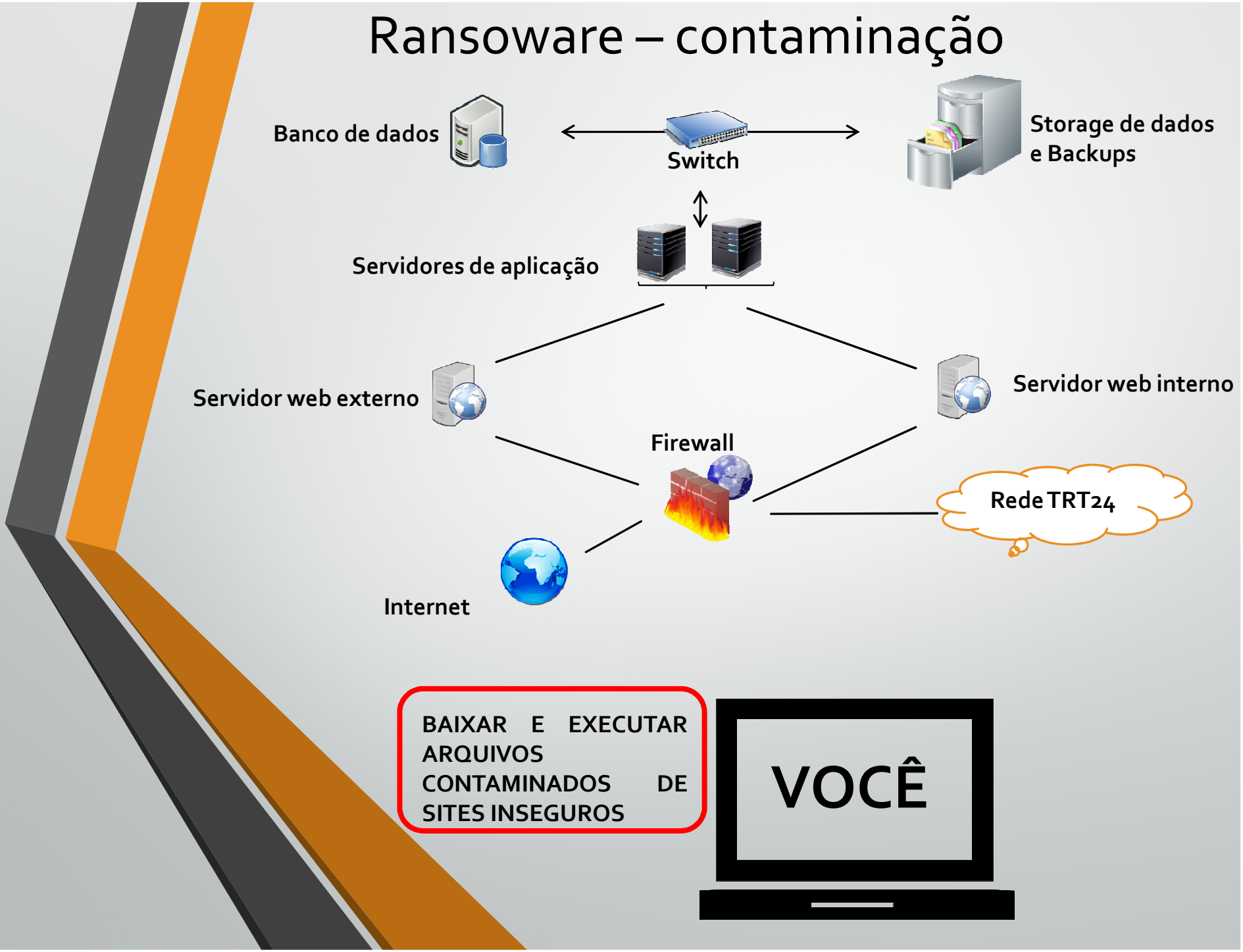


NÃO VERIFICAR SE ANTIVÍRUS E WINDOWS ESTÃO COM AS ÚLTIMAS ATUALIZAÇÕES

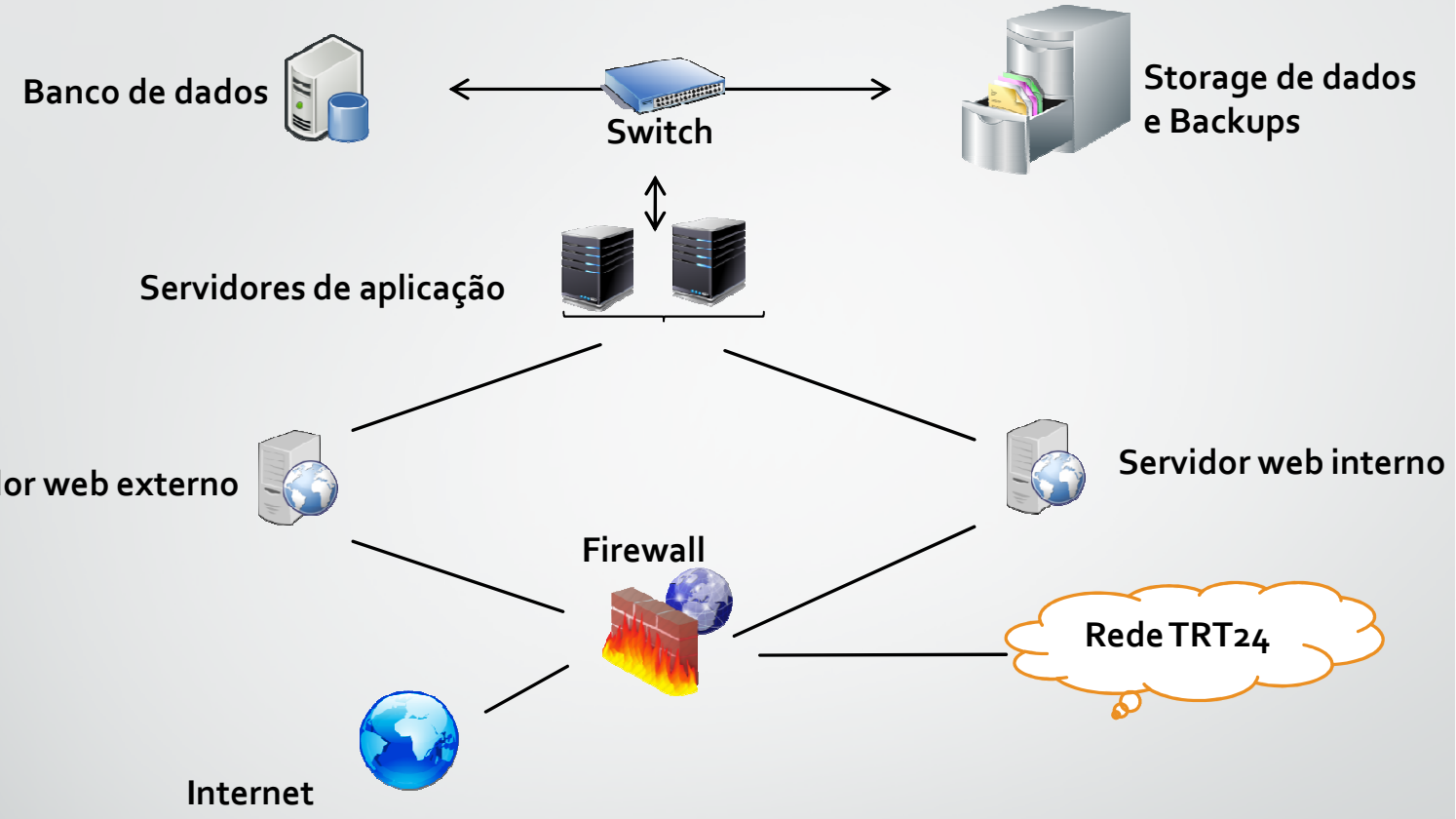
Ransoware – contaminação



Ransoware – contaminação



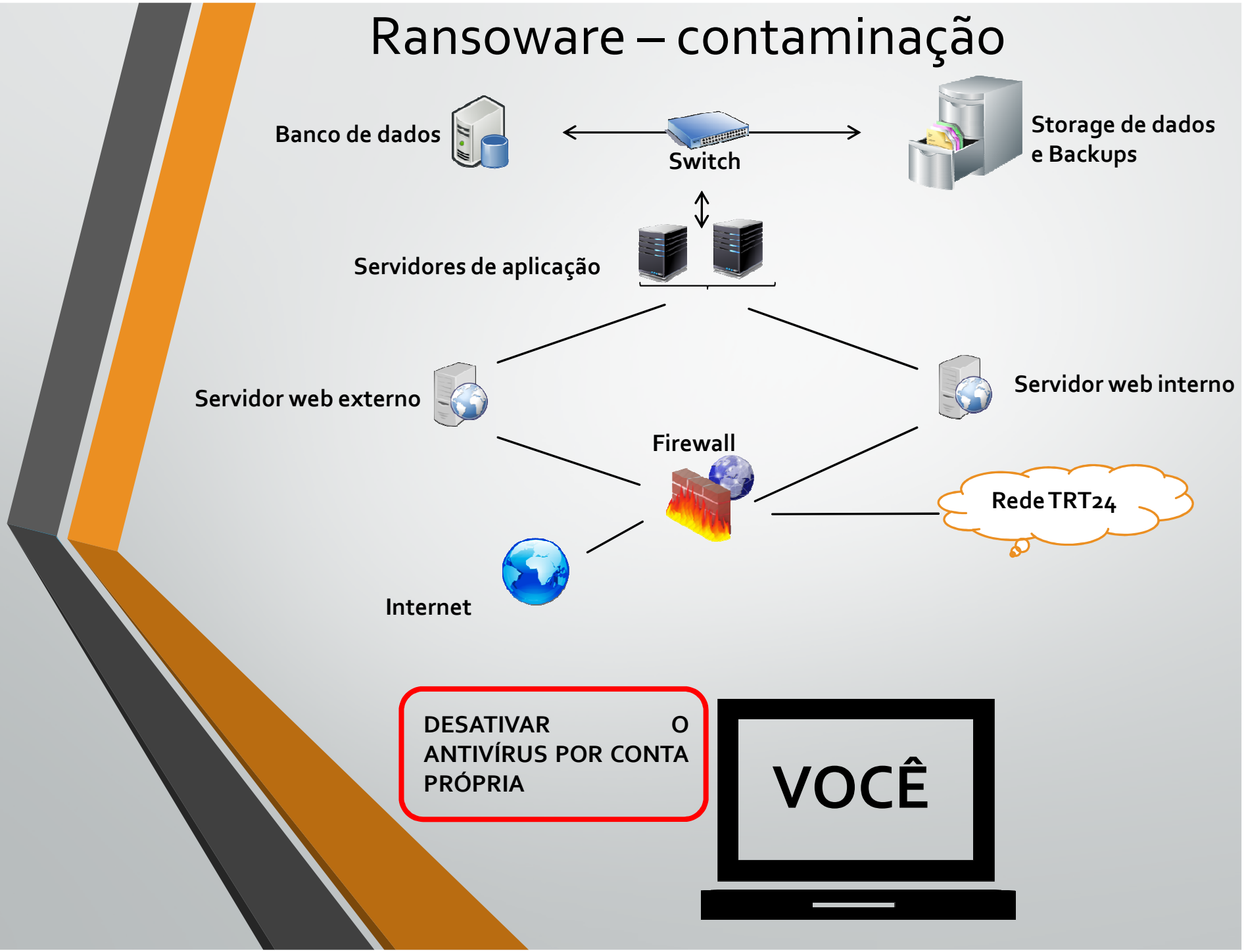
Ransoware – contaminação



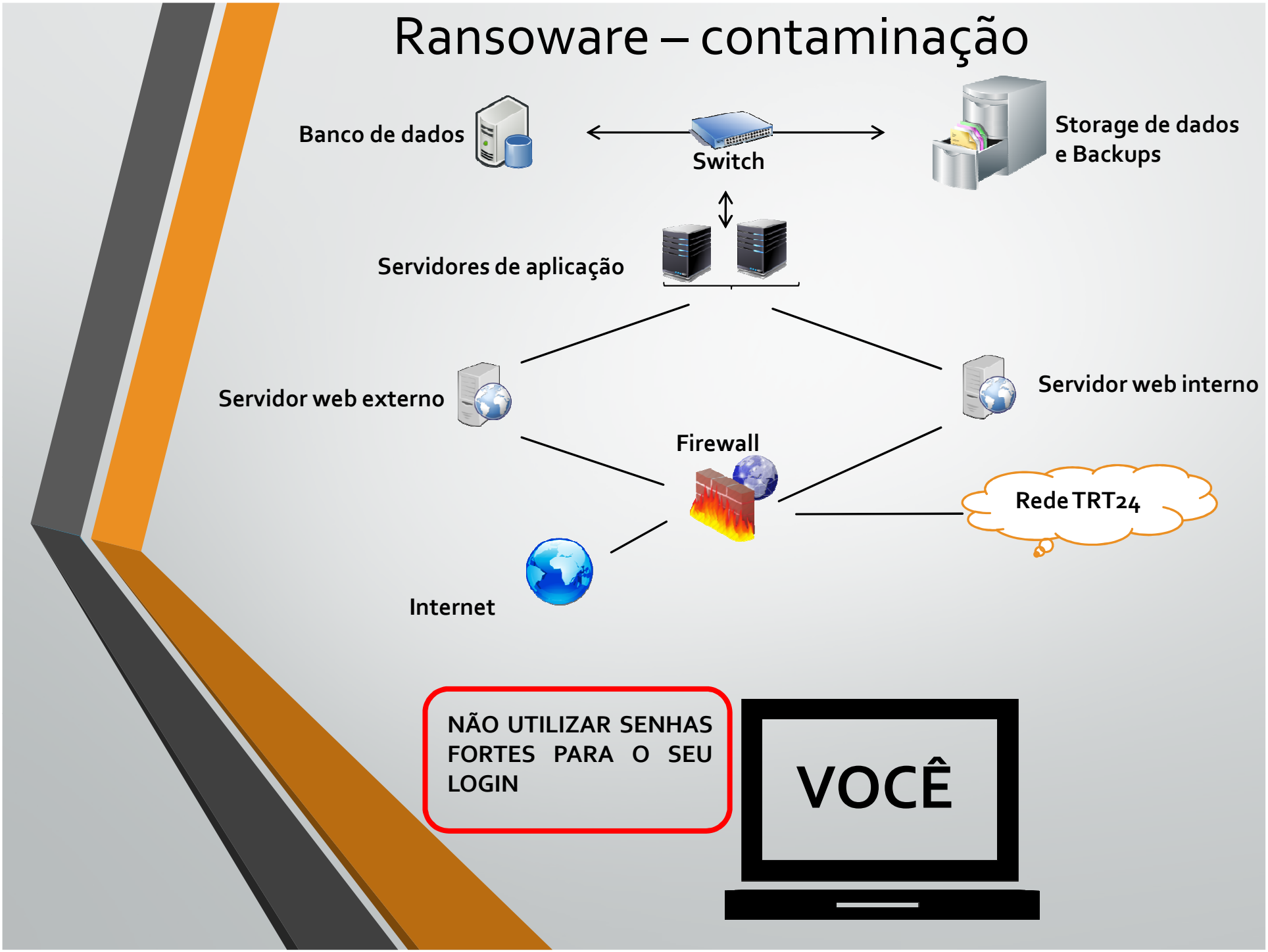
INSTALAR SOFTWARES SEM O ACOMPANHAMENTO DA TI

VOCÊ

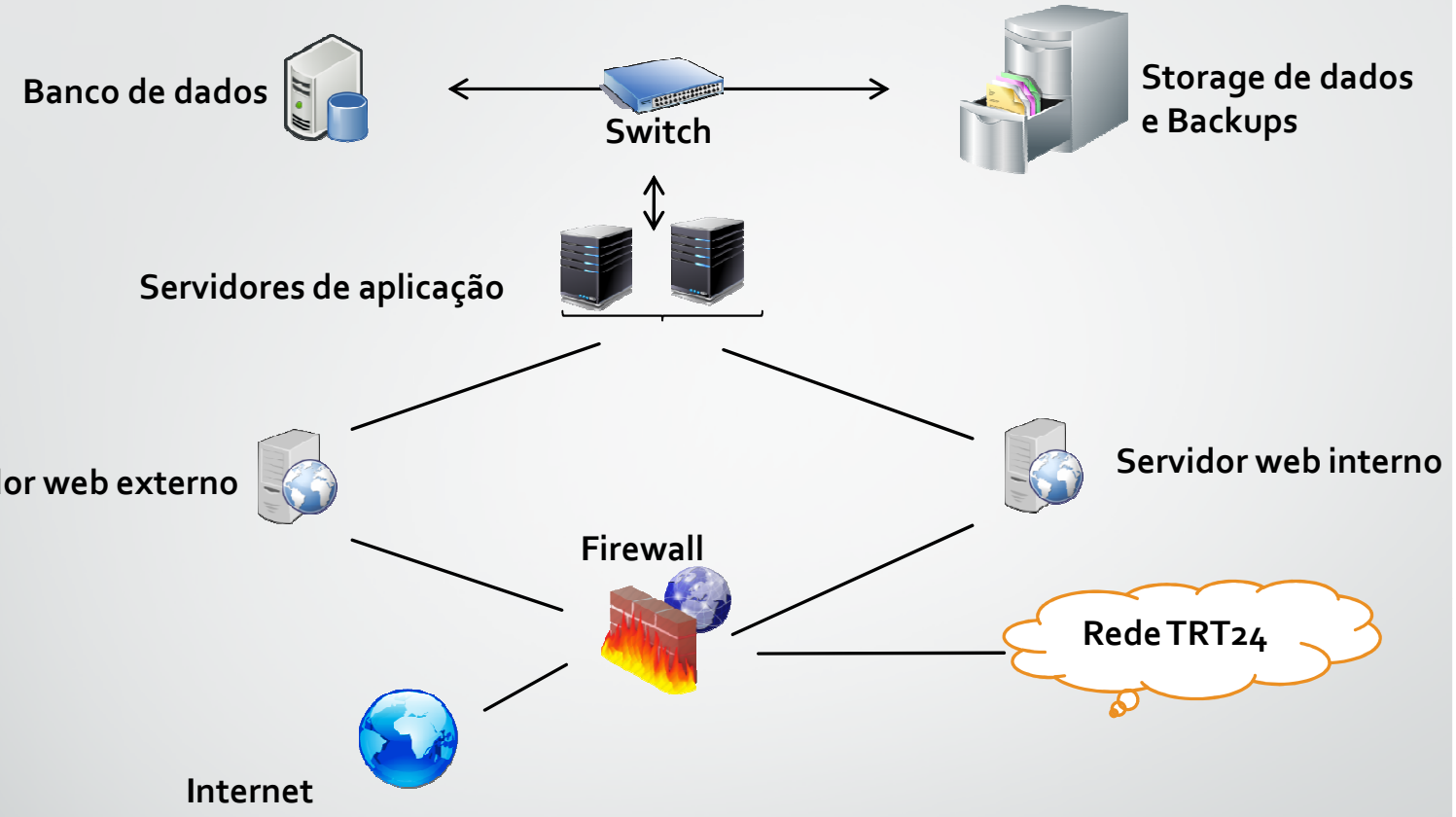
Ransoware – contaminação



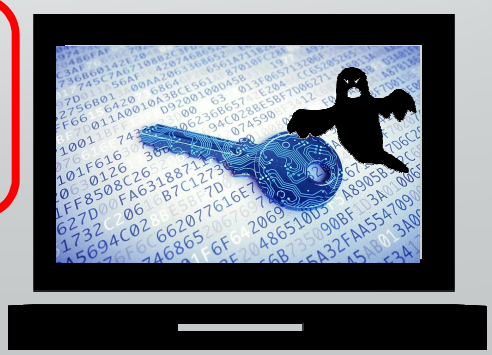
Ransoware – contaminação



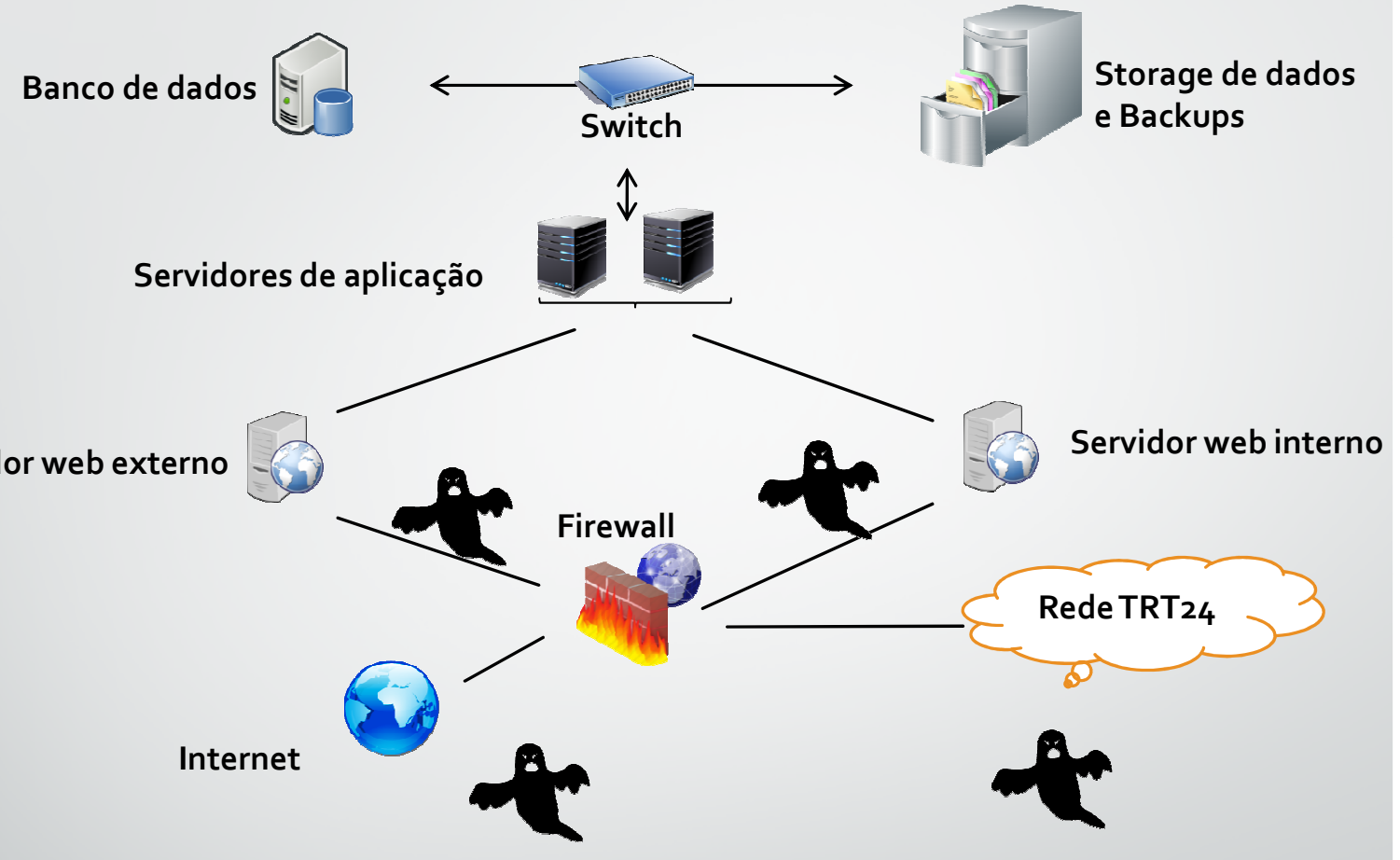
Ransoware – contaminação



RANSOWARE CRIPTOGRAFA DADOS LOCAIS DA SUA ESTAÇÃO

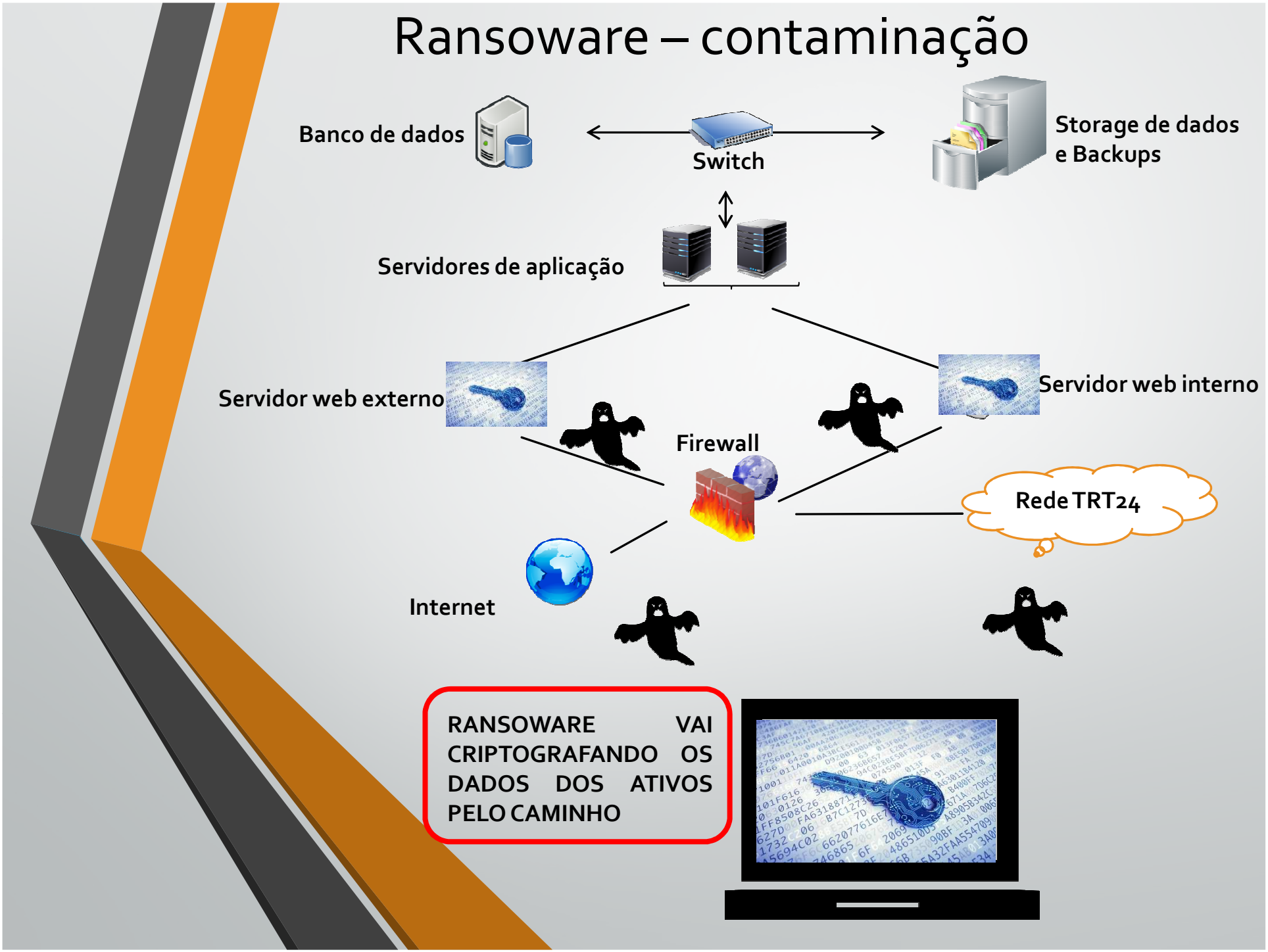


Ransoware – contaminação

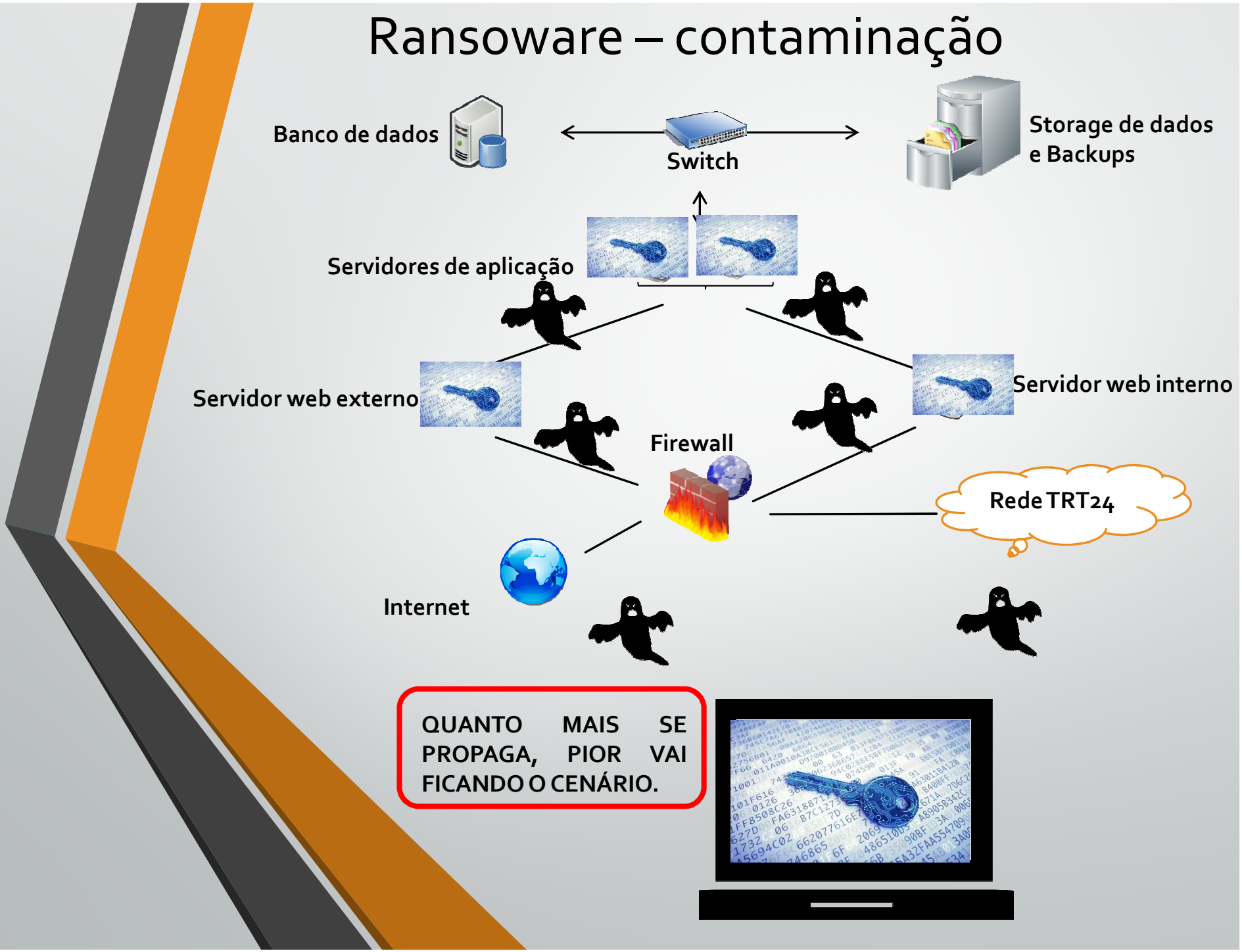


RANSOWARE SE PROPAGA PELA REDE ATRAVÉS DE ALGUMA VULNERABILIDADE SEM ATUALIZAÇÃO

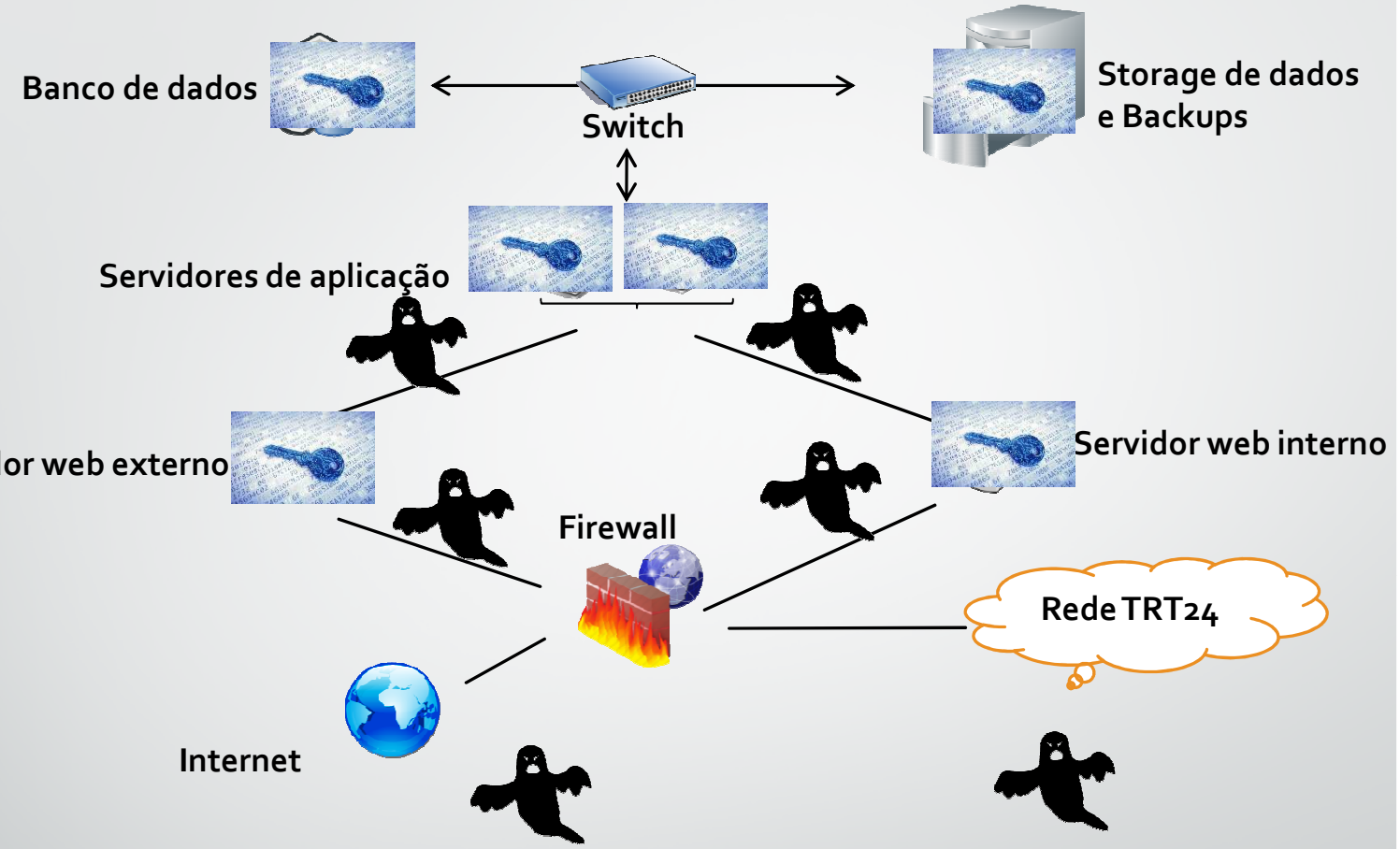
Ransoware – contaminação



Ransoware – contaminação

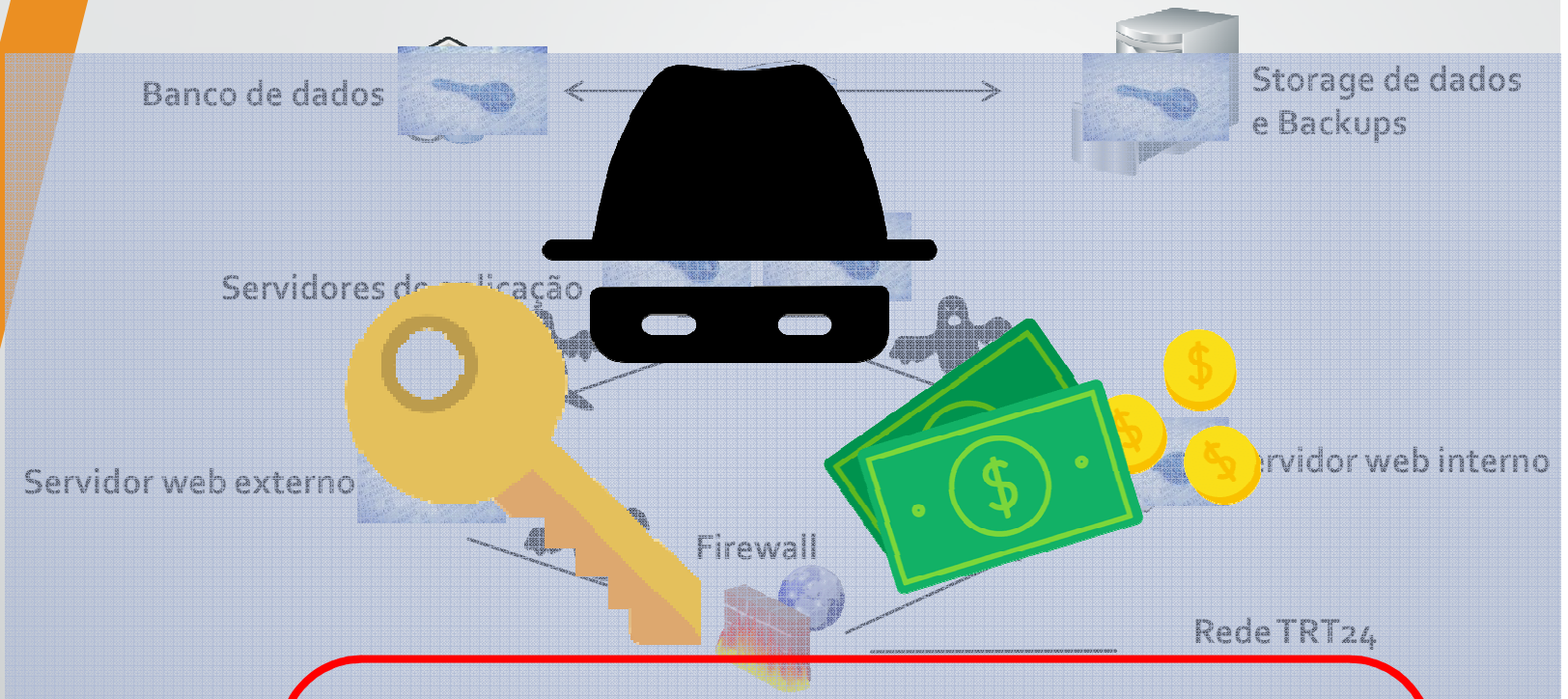


Ransoware – contaminação



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

Ransoware – contaminação



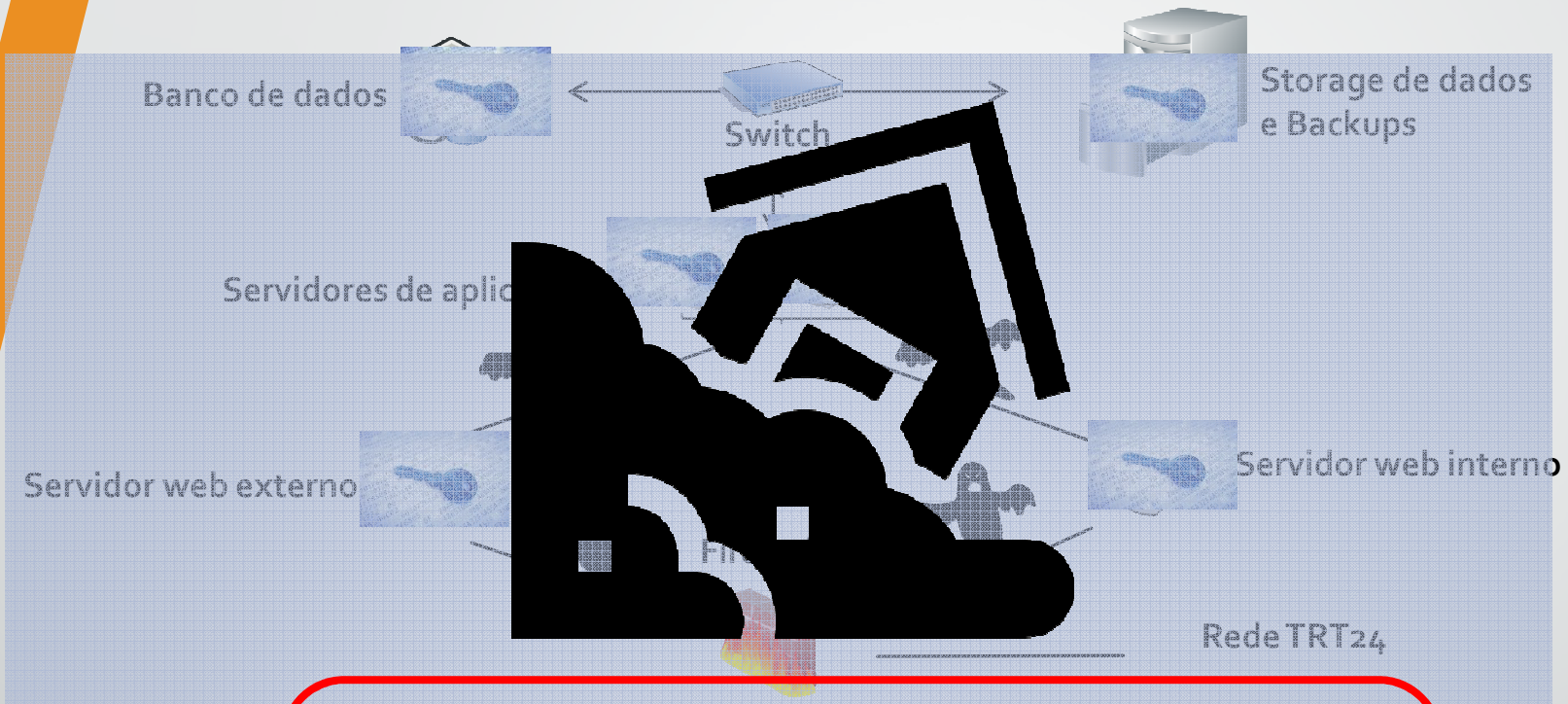
-NO FINAL DE TUDO, O ATACANTE PEDE RESGATE EM TROCA DA CHAVE CAPAZ DE RECUPERAR AS INFORMAÇÕES.

-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.

Ransoware – 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 - <u>senhas fracas</u>**

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:**

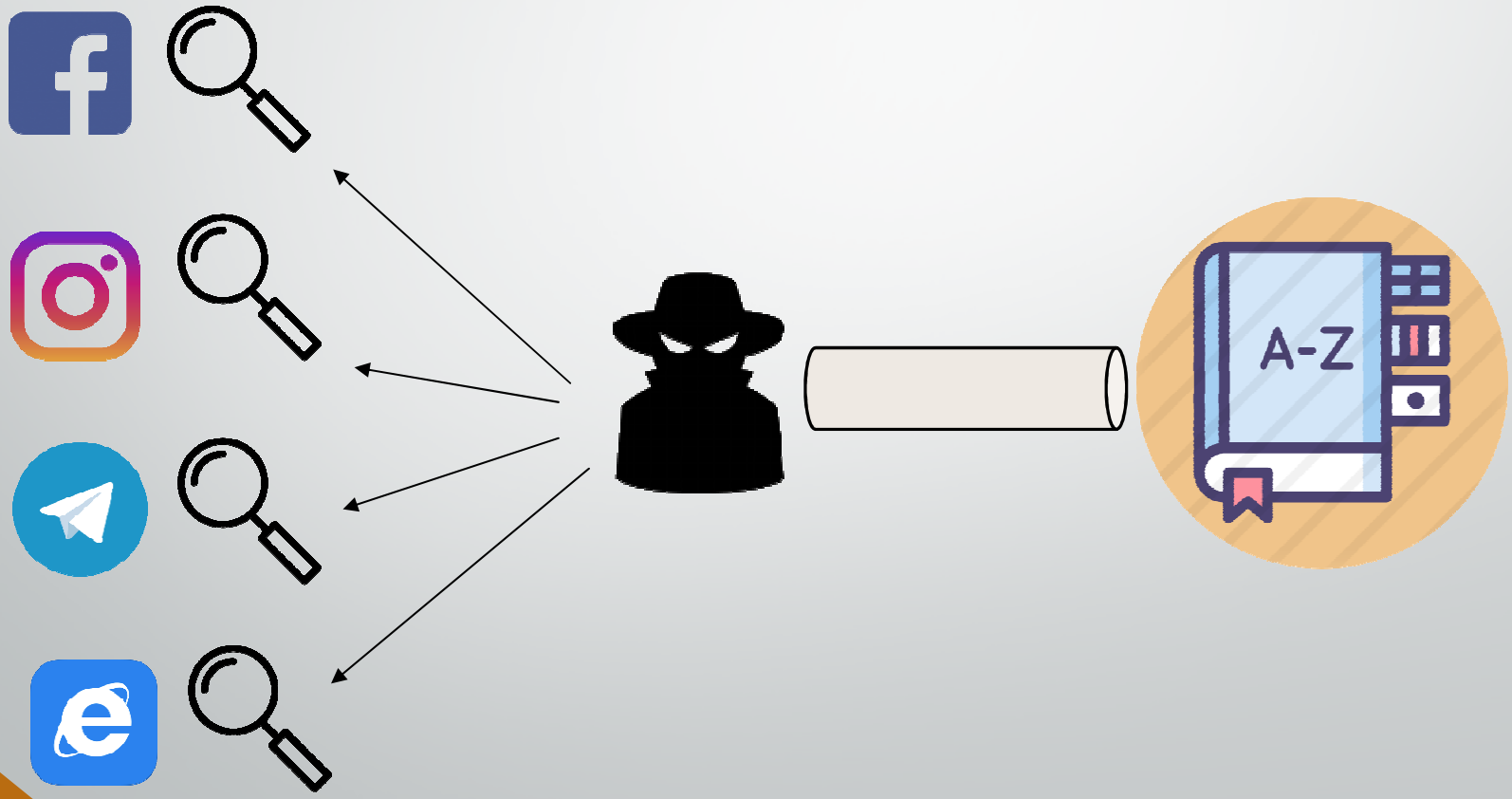
   - Método para confeccionar senhas fortes:

     - 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

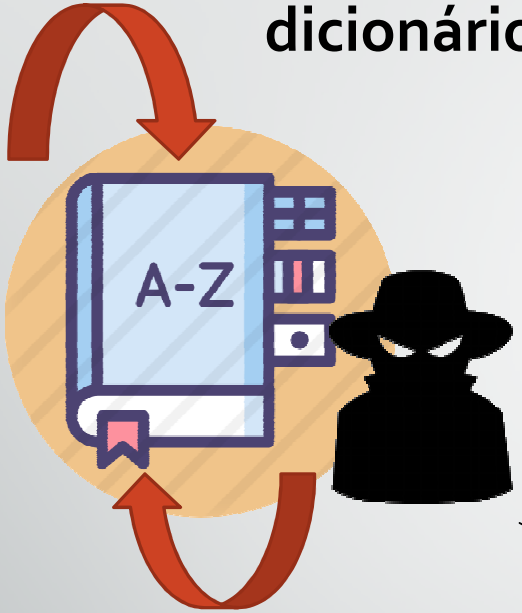
- Engenharia social

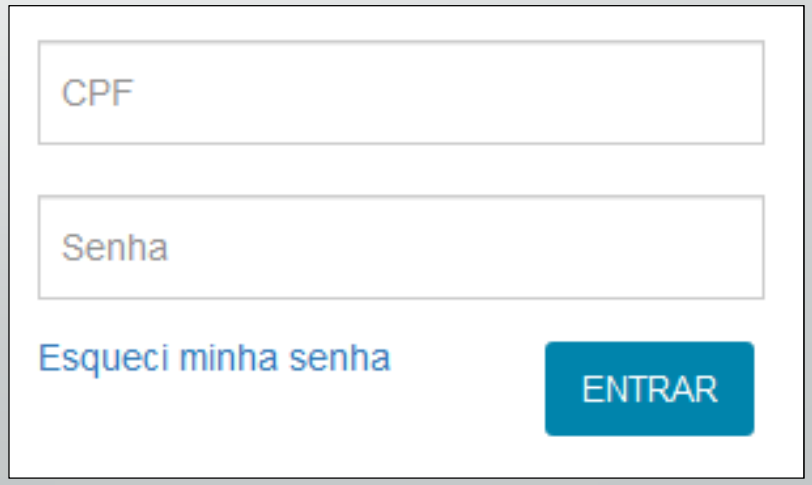
4. Quebra de senhas: **Ataque de dicionário - <u>senhas fracas</u>**



- Engenharia social

4. Quebra de senhas: **Ataque de dicionário - <u>senhas fracas</u>**





- Engenharia social

  4. Quebra de senhas: **Ataque de dicionário – <u>contramedidas</u>**

     - 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

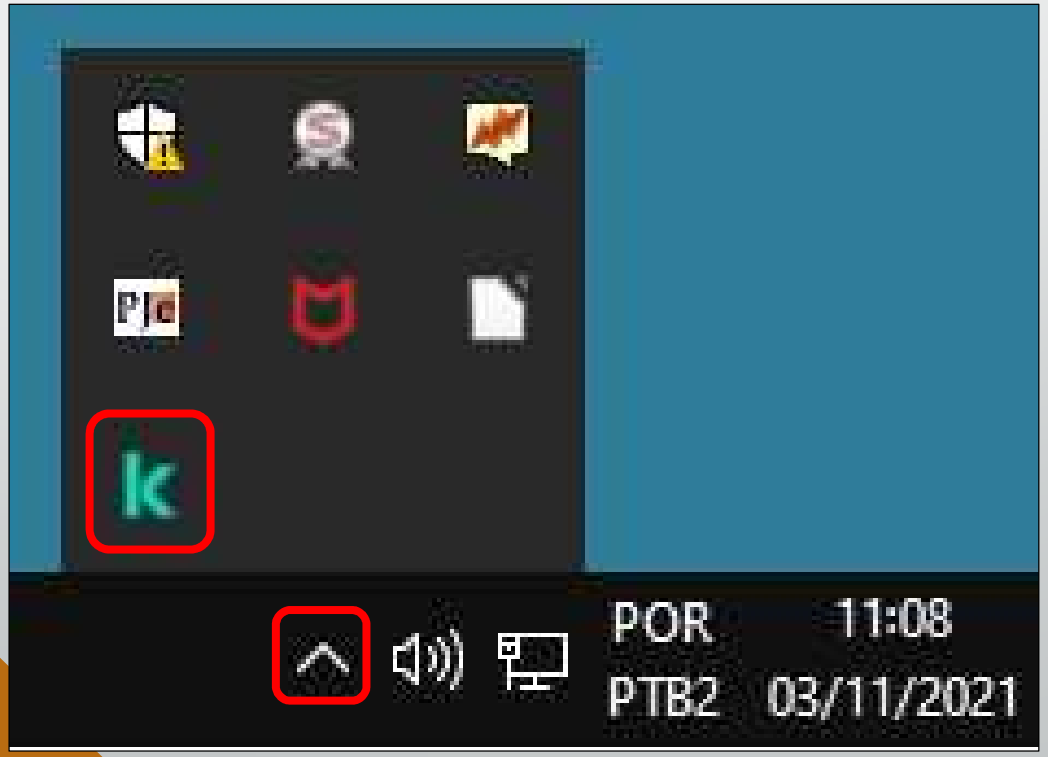
1. Verificar se o seu antivírus está atualizado e funcionando (Rede interna TRT24)
   - A partir do dia 09/11/2021, iniciaremos o processo de migração de antivírus da **Mcafee** para a solução recém adquirida da **Kaspersky**;
   - Muito importante que todas as máquinas estejam ligadas e logadas para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

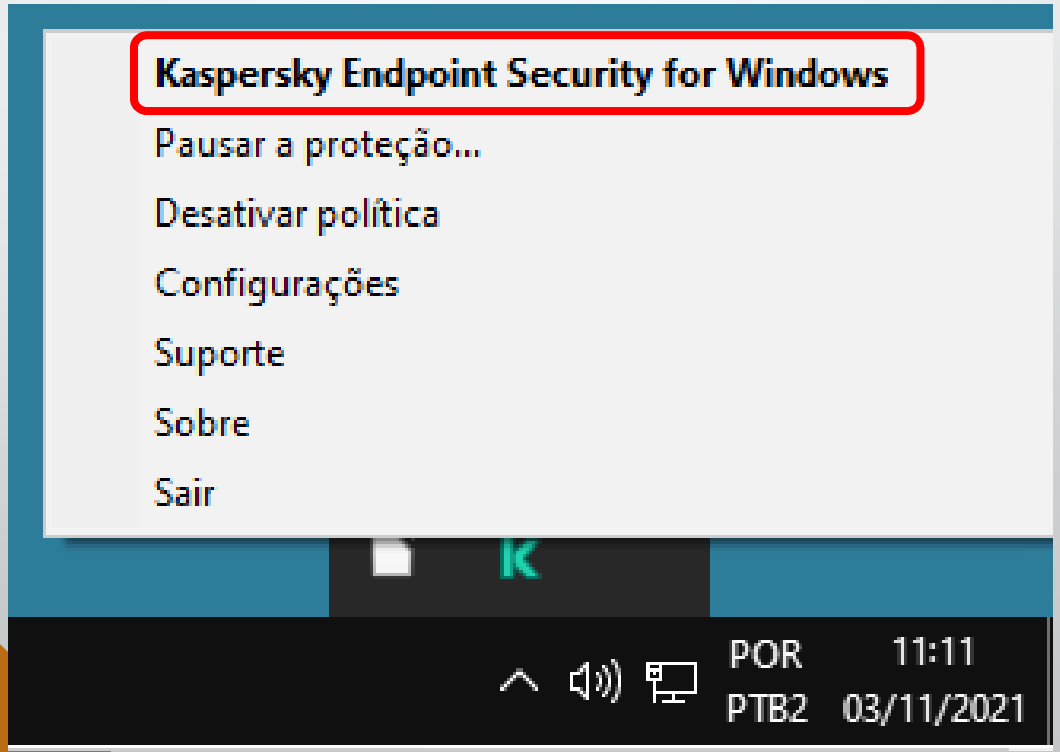
Semana da Segurança da Informação – Ações

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



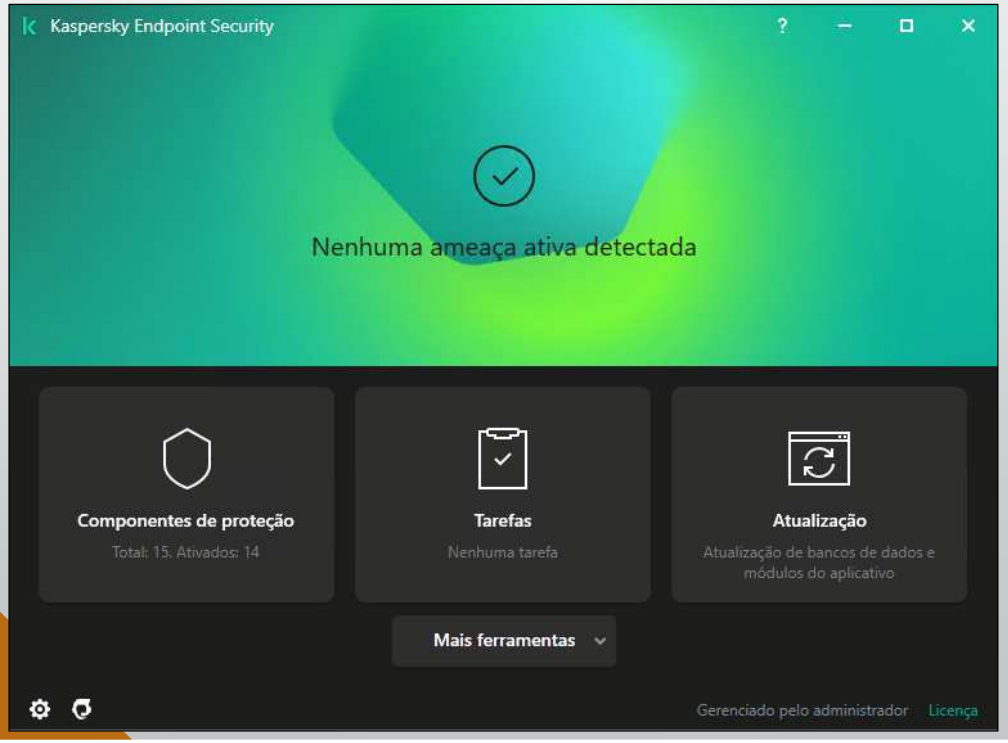
Semana da Segurança da Informação – Ações

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 ? **<u>Abrir SIATE imediatamente</u>** 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

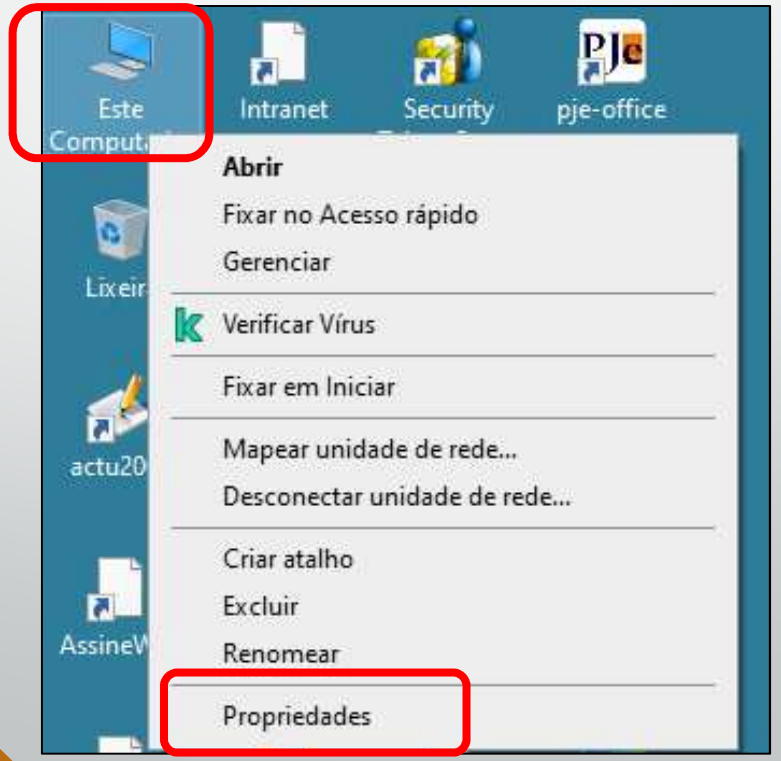
Semana da Segurança da Informação – Ações

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

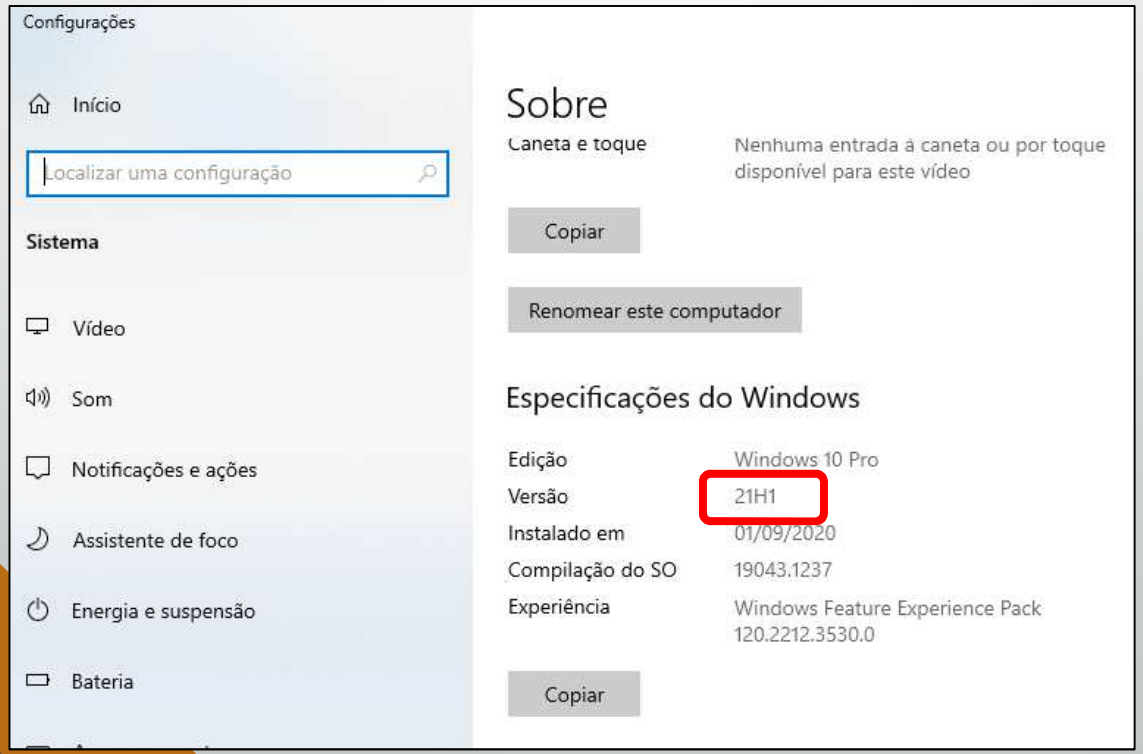
Semana da Segurança da Informação – Ações

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



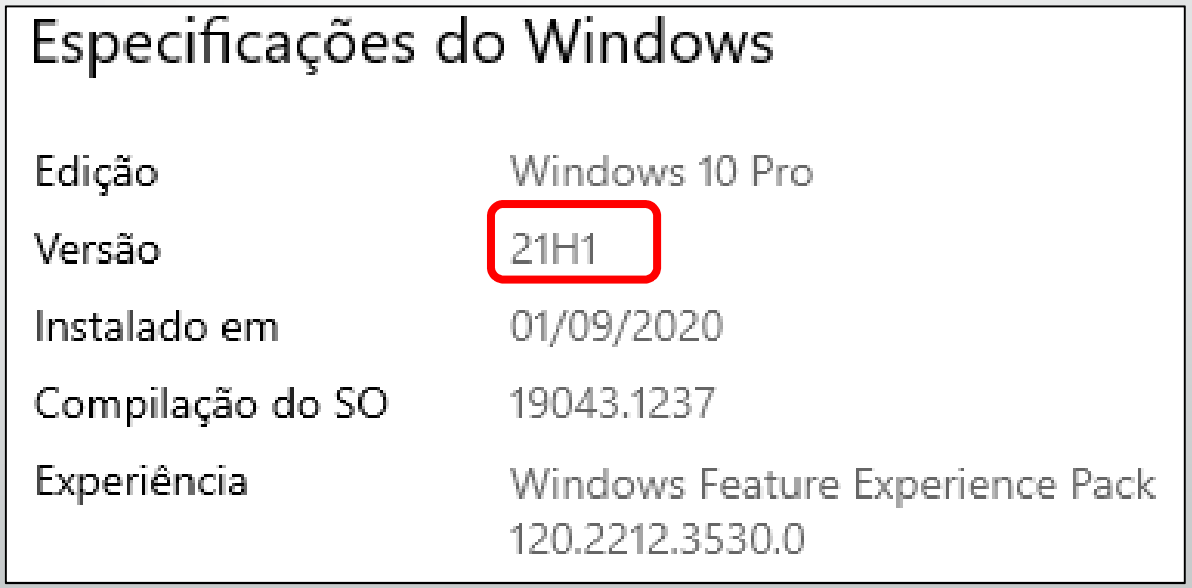
Semana da Segurança da Informação – Ações

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



Semana da Segurança da Informação – Ações

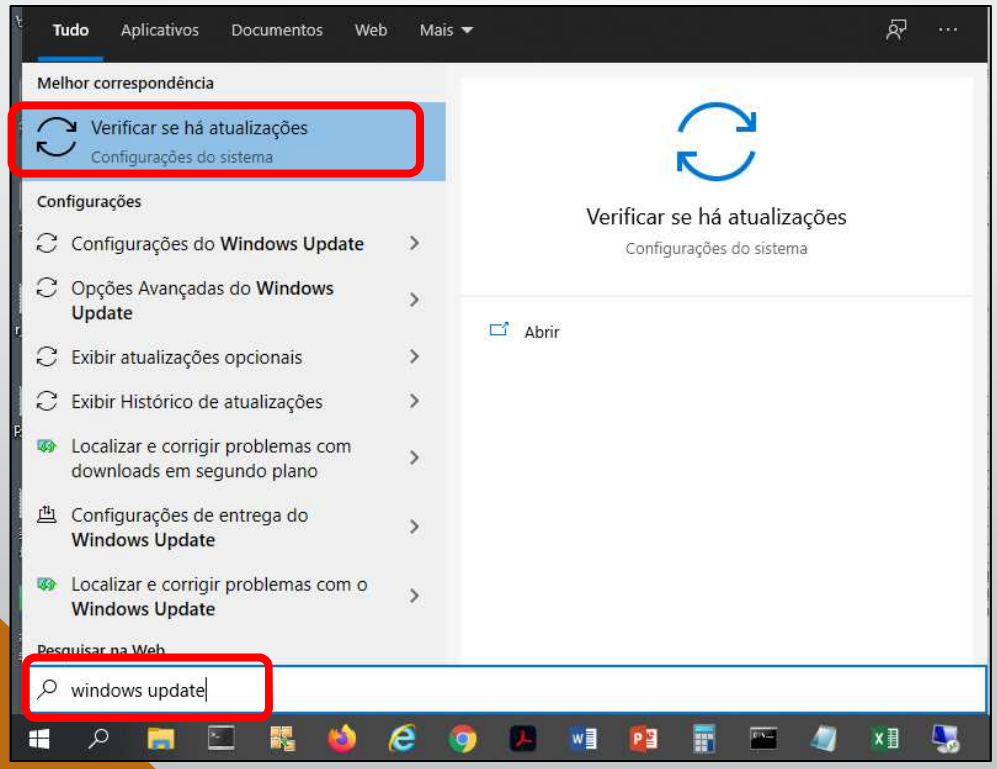
2. Verificar se o seu Windows está atualizado e na última versão;
   - Como verificar a versão do seu Windows:



Semana da Segurança da Informação – Ações

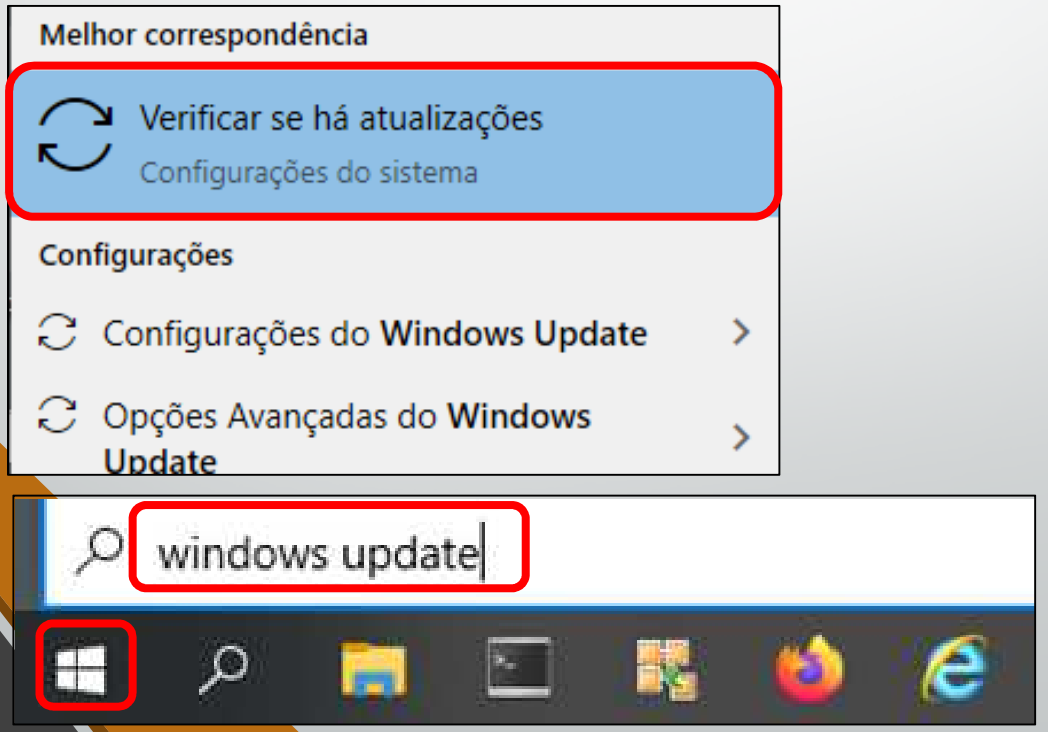
2. Verificar se o seu Windows está atualizado e na última versão;

   - Como verificar se Windows está atualizado:



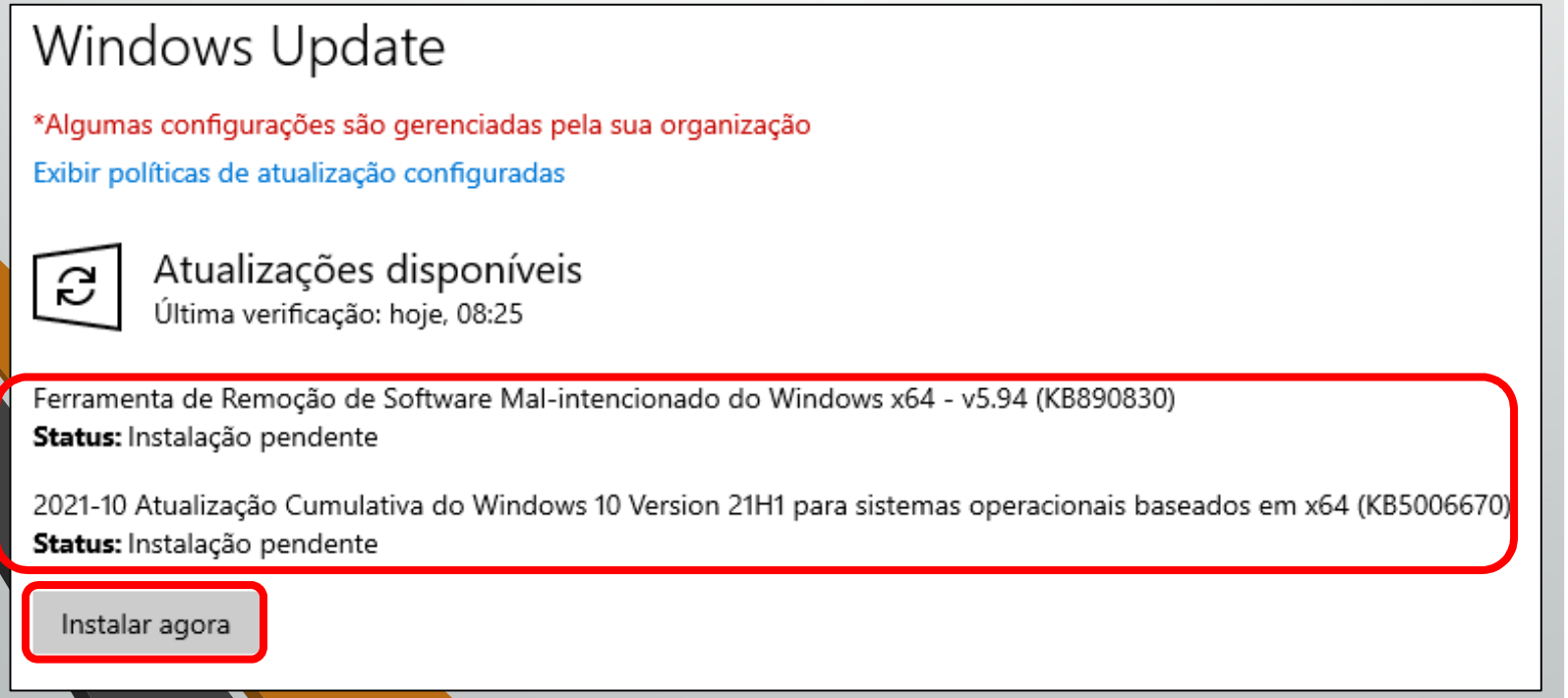
Semana da Segurança da Informação – Ações

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



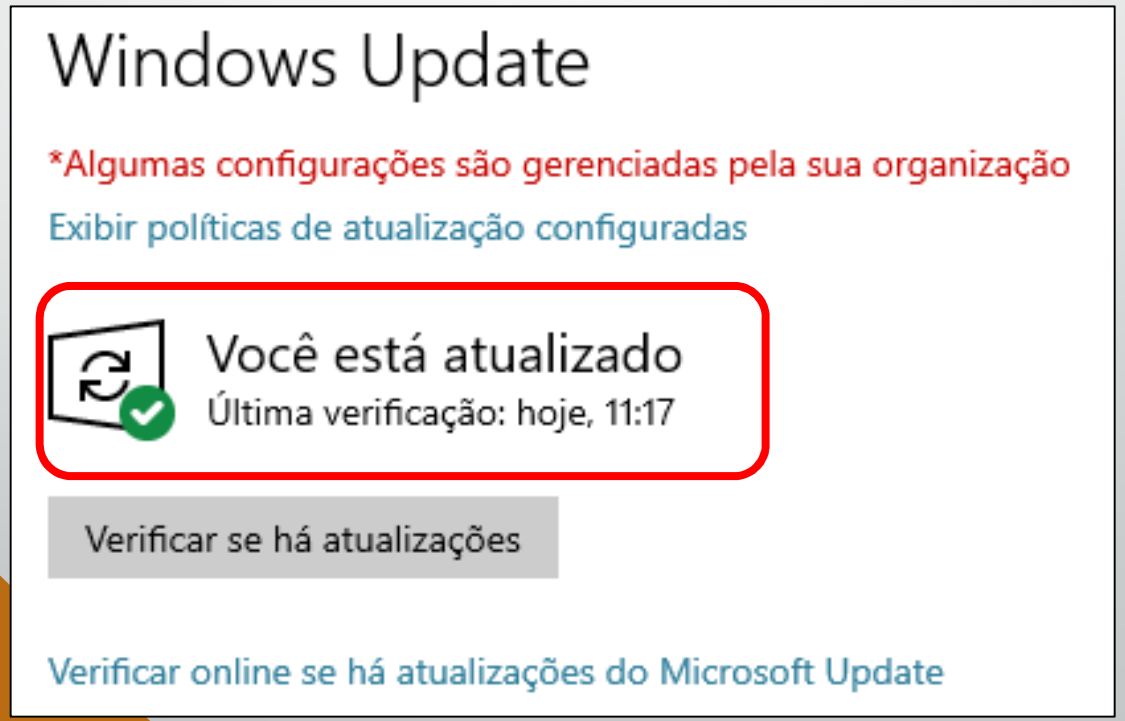
Semana da Segurança da Informação – Ações

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



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

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

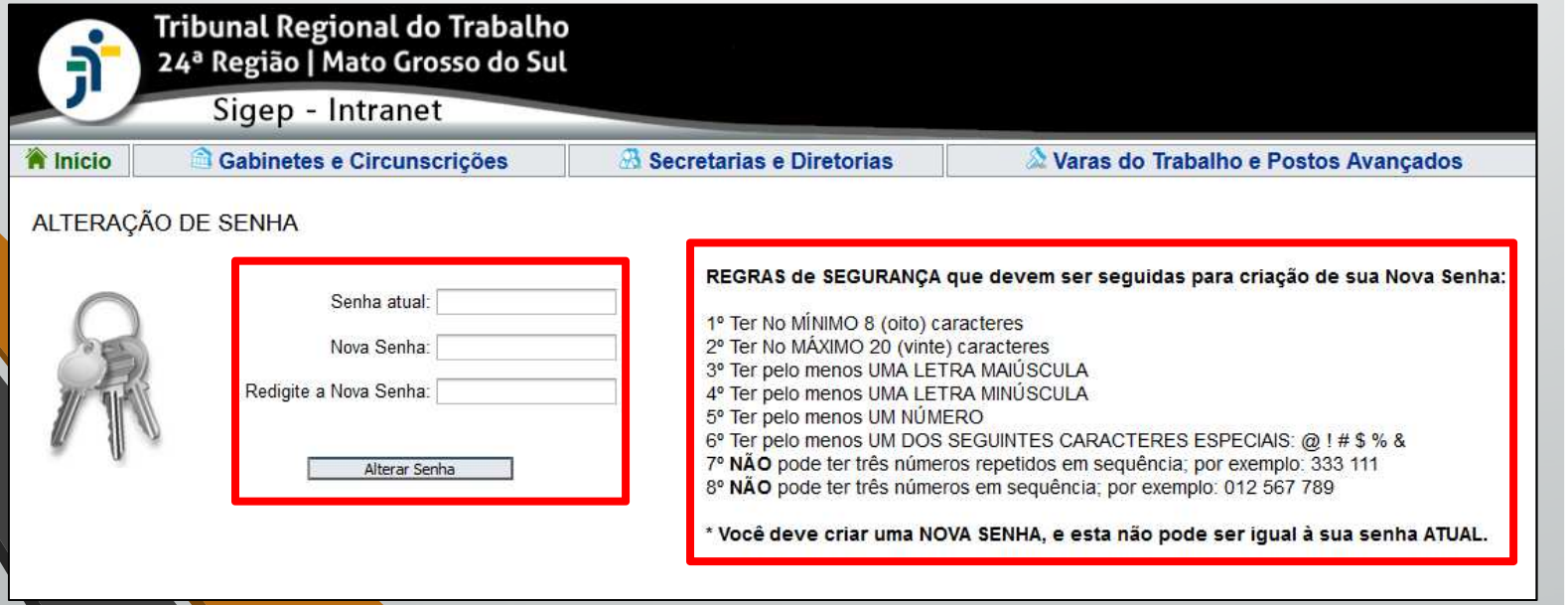
3. Mudar sua senha na Intranet
   - Como trocar a senha: acesse https://intranet.trt24.jus.br

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"



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.

Semana da Segurança da Informação – Ações

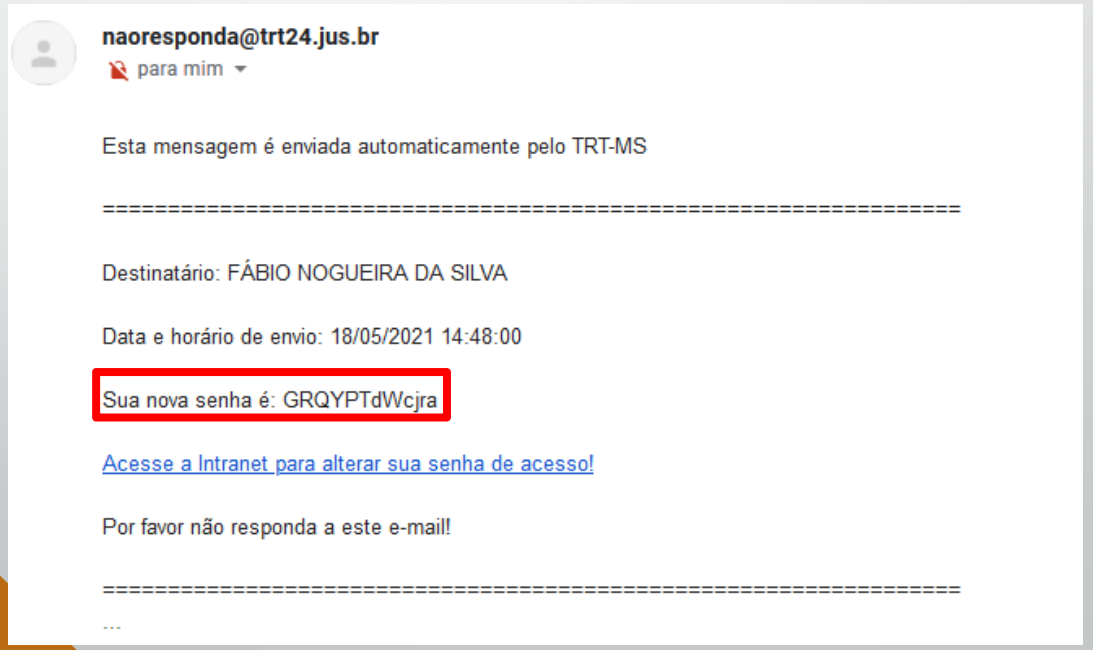
3. Mudar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha até o vencimento:
        - Caso possua e-mail de recuperação cadastrado: na janela que aparecer, preencher o campo CPF, Captcha, data de nascimento e clicar no botão "Solicitar nova senha".

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.

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

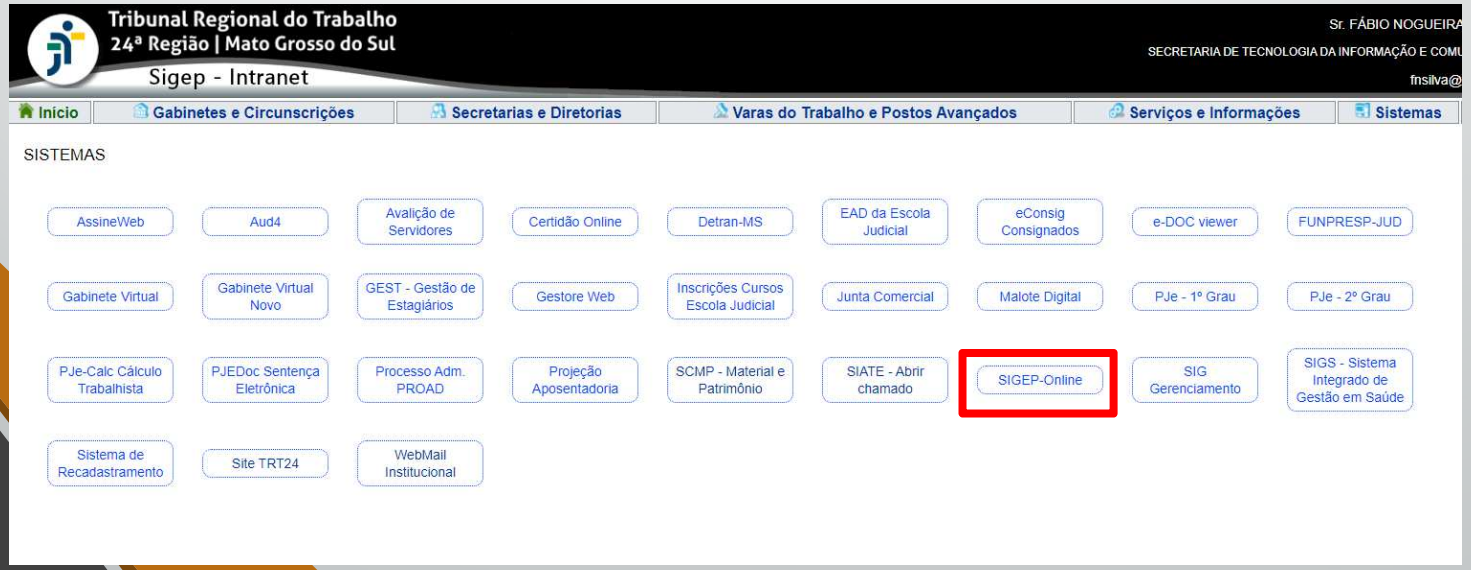
3. Mudar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha até o vencimento:
        - Se não possuir e-mail de recuperação cadastrado: **é possível se cadastrar no SIGEP-Online.** Para isso:
            - Entre na nossa intranet em https://intranet.trt24.jus.br

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

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



Semana da Segurança da Informação – Ações

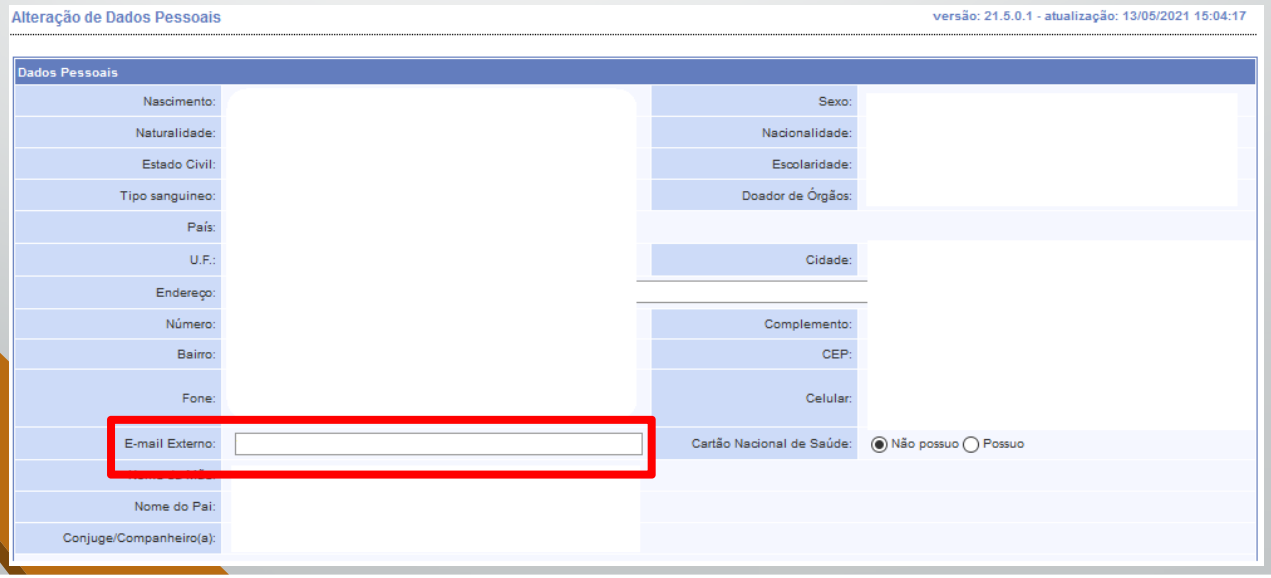
3. Mudar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha até o vencimento:
        - Se não possuir e-mail de recuperação cadastrado: **é possível se cadastrar no SIGEP-Online.** Para isso:
            - Você será direcionado à tela inicial do SIGEP-Online. Basta se logar nessa tela com seu usuário e senha.

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"

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.



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/