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

Segurança da Informação

Protocolos para prevenção de incidentes cibernéticos

Fábio Nogueira da Silva

Equipe da Seção de Segurança da Informação

SETIC

Conteúdo

1. O que é a Informação
2. Proteção da Informação
   - Nível organizacional
   - Nível individual
3. Segurança física e lógica;
4. Ataques à segurança física;
5. Ataques à segurança lógica;
6. Semana da Segurança da Informação
   - O que a SETIC vai fazer
   - O que você precisará fazer

O que é a informação?

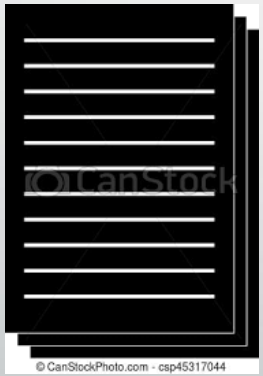
- O ativo estratégico mais importante de uma organização.

- É um conjunto de conhecimento organizado pertencente a determinada organização, podendo ser de domínio público ou privado.

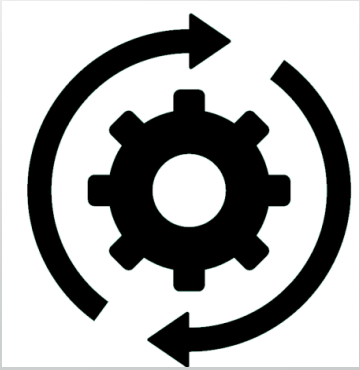
Distribuição da informação

Pessoas

Equipamentos de TI



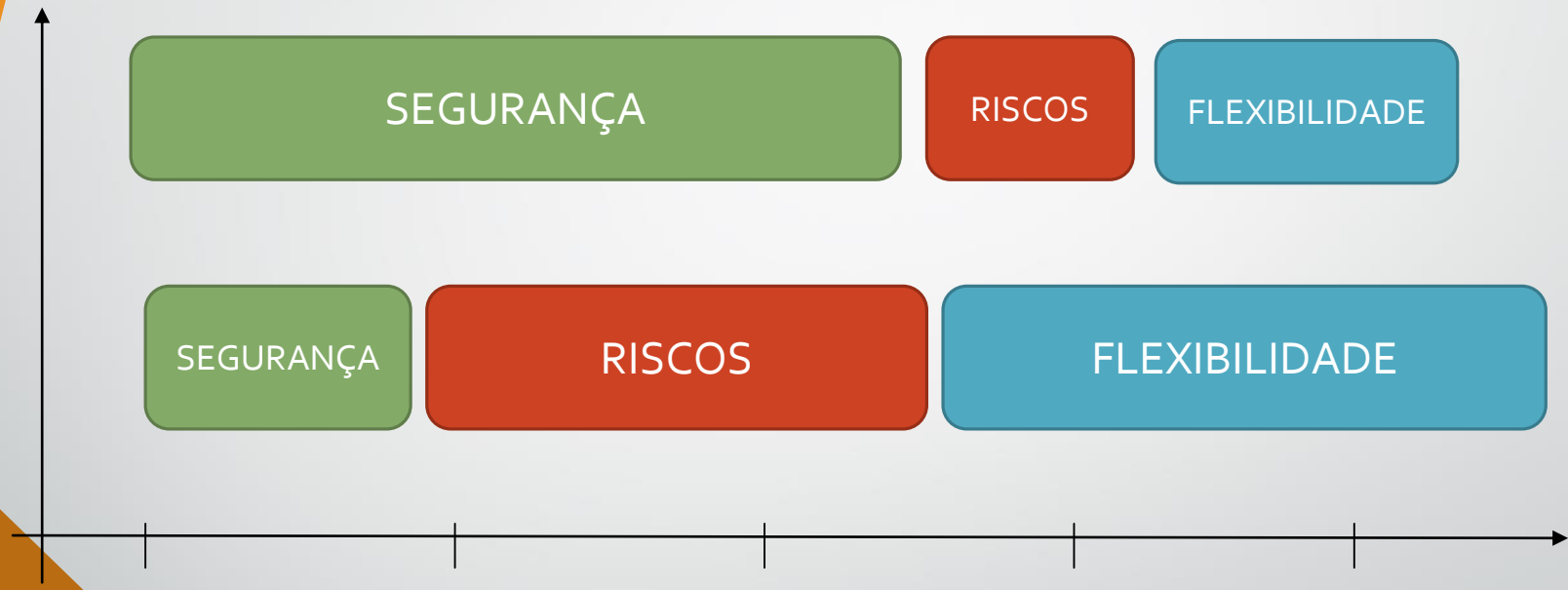
Papéis e documentos



Sistemas e processos de trabalho

Precisamos proteger a informação

Desafios para proteção da informação



Níveis de Segurança, Risco e Flexibilidade

Proteção da informação

- Nível organizacional
- Nível pessoal

Proteção da informação a nível organizacional

Políticas de Segurança da Informação

Comitê de Segurança da Informação

Normas externas, boas práticas em SI ...

Juiz Indicado da Presidência
Diretor(a) Geral
Diretor(a) da SJ
Diretor(a) da SETIC
Chefe da Seção de Segurança

Políticas de Segurança da Informação

Normas externas, boas práticas em SI ...

Comitê de Segurança da Informação

Juiz Indicado pela Presidência
Diretor (a) Geral
Diretor(a) da SJ
Diretor(a) da SETIC
Chefe da Seção de Segurança

Processos de SI

Ger. Ativos

Ger. de Riscos

Ger. Continuidade

Ger. Incidente de SI

Ger. Acessos

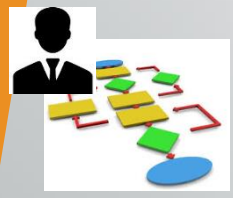
Políticas de Segurança da Informação

Normas externas, boas práticas em SI ...

Comitê de Segurança da Informação

Juiz Indicado da Presidência
Diretor-(a)Geral
Diretor(a) da SJ
Diretor(a) da SETIC
Chefe da Seção de Segurança

Processos de SI



Ger. Ativos

Ger. de Riscos

Ger. Continuidade

Ger. Incidente de SI

Ger. Acessos

Projetos

Projetos ciclo 2021-2022

- Adquirir ferramenta de Gestão de Riscos
- Implantar LGPD
- Contratar Solução de Antivírus
- Aprimorar Processo de Segurança da Informação
- Implementar proxy através do firewall
- Contratar suporte para solução de backup
- Implantar ferramenta(s) de pesquisa de vulnerabilidades
- Aprimorar monitoramento de incidentes de SI
- Aprimorar registros de acessos (logs)

Proteção da informação a nível organizacional

- É suficiente ???

Proteção da informação a nível organizacional

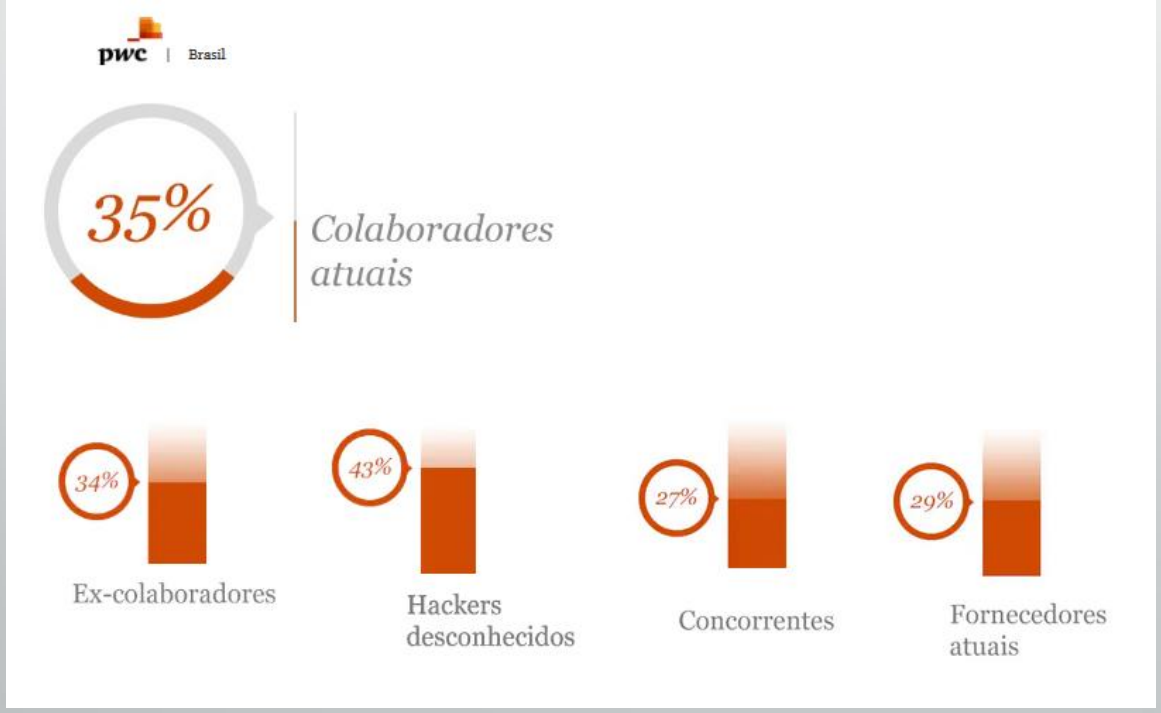
- É suficiente ???

NÃO


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 ?

- Diversos ataques recentes a órgãos públicos com o crescimento do trabalho remoto:
  - TJ/RS – 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

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

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

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.

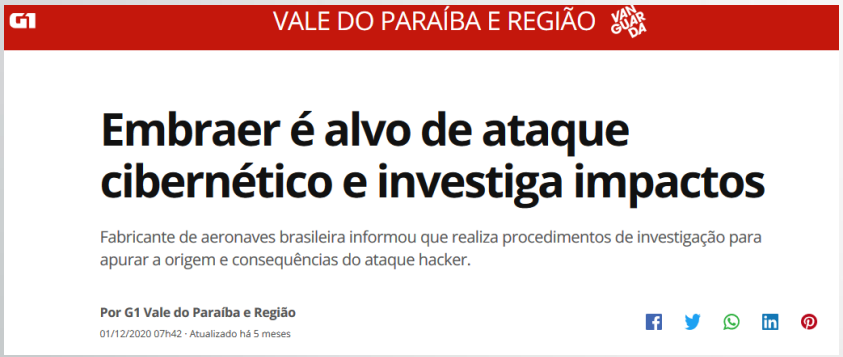
Por G1 São Paulo

12/05/2017 15h45 · Atualizado há 4 anos

Por que você é tão importante ?

- Notícias recentes de ataques cibernéticos

01/12/2020



10/05/2021

24/02/2021

19/05/2021

Proteção da informação a nível individual

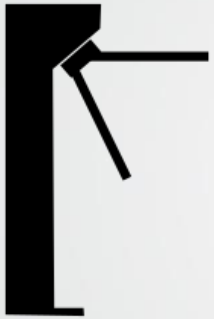
Proteção da informação a nível individual

- Áreas da Segurança da Informação
  1. Segurança física
  2. Segurança lógica

Segurança física

- Corresponde a construção de barreiras de forma a evitar ou retardar intrusões físicas, garantindo uma resposta eficaz.
- Prevenção de desastres locais ou ambientais.

Exemplos



Catracas de acesso

Área de recepção

Equipe de vigilantes

Crachá de acesso

Cancelas no estacionamento

Câmeras de segurança

Botão de pânico

Detector de metais

Como você pode ajudar?

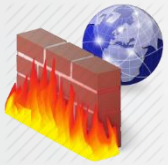
- Ficar atento ao movimento de pessoas estranhas e sem identificação no ambiente de trabalho.
- Acompanhar terceiros autorizados durante o acesso físico a ambiente interno do TRT.
- Somente pessoas autorizadas ou acompanhadas pela SETIC podem acessar perímetros críticos:
    - Sala cofre.
    - Salas técnicas do Fórum, Sede e Interior.

Segurança lógica

- Mecanismos e dispositivos para controlar o acesso a aplicativos, dados, computadores e notebooks.

Segurança lógica

- Dispositivos e mecanismos de segurança dentro da TI



Firewall de rede

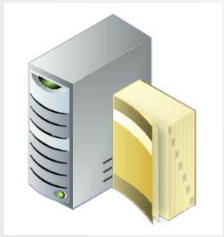
Controle de portas nos switches

Proxy de navegação

Sistemas de detecção de intrusão

Segurança lógica

- Dispositivos e mecanismos de segurança nos computadores dos usuários



Políticas de senhas do domínio

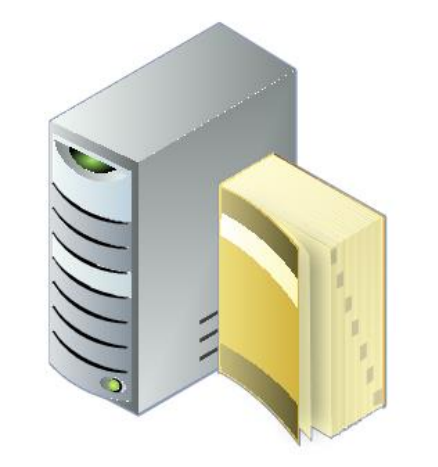
Antivírus

Políticas da mesa limpa

Windows update

Segurança lógica

Política de senhas do domínio



Segurança lógica

Política de senhas do domínio

- Trocas obrigatórias a cada 6 meses;
- Tamanho mínimo de 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 (cpf, rg, login, nome, data de aniversário);
- Não anotar a senha em papel;

Segurança lógica

Política de senhas do domínio

- **Conceito de senhas fortes mudou ao longo do tempo.**
- **O importante é não anotar em papel e não compartilhar a sua senha;**
- **Dicas na hora de trocar a senha:**

1. Escolha uma frase de que goste;
2. Escolha um ou mais números de que goste;
3. Escolha um ou mais dos seguintes caracteres especiais: @ ! # $ % &
4. Posicione os números nos espaços da frase e o caractere especial substituindo o último espaço;

Segurança lógica

- Política de senhas do domínio

- **Exemplo passo 1 – escolha uma frase de que goste:**

  "Penso logo existo"

Segurança lógica

- Política de senhas do domínio

- **Exemplo passo 2 – escolha uma número de que goste:**

6

Segurança lógica

- Política de senhas do domínio

- **Exemplo passo 3 – escolha um caractere especial:**

@

Segurança lógica

- Política de senhas do domínio

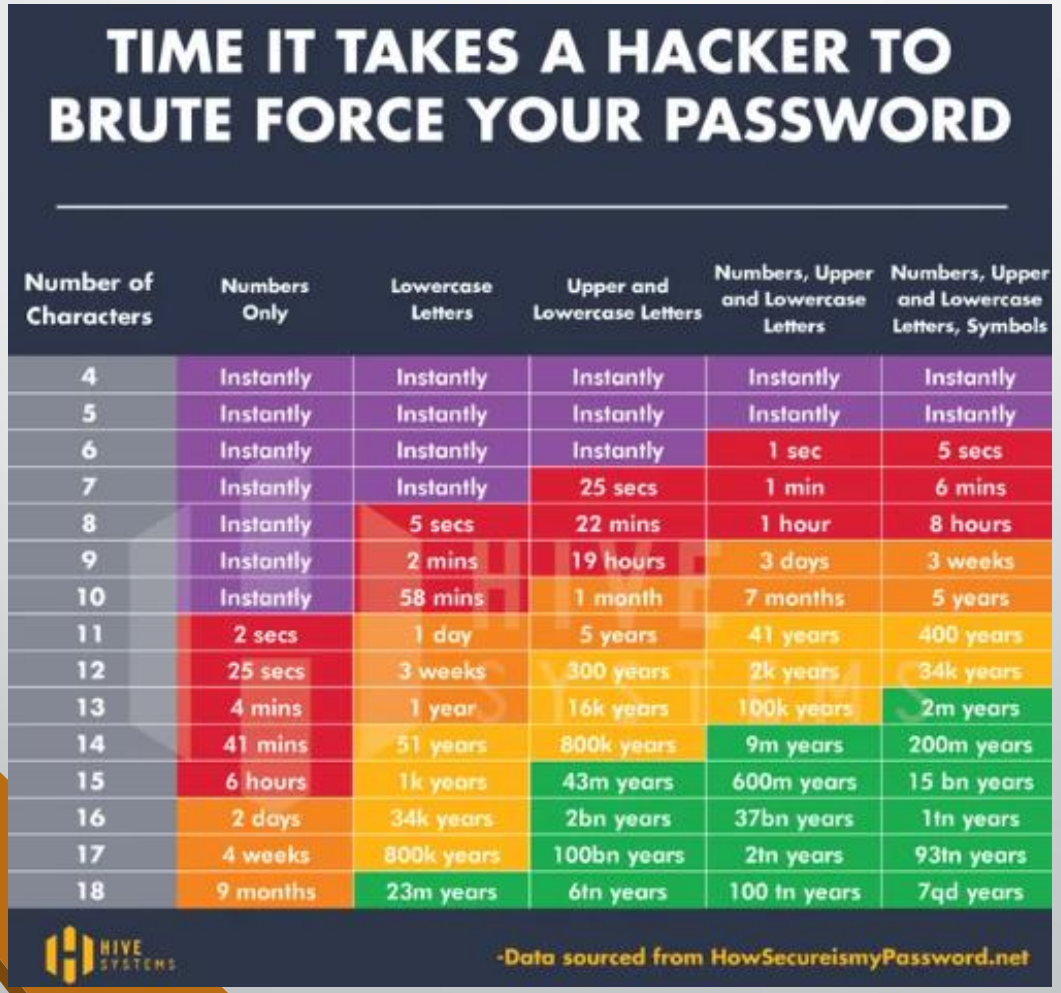
- **Exemplo passo 4 – posicione o numero nos espaços da frase e o caractere especial substituindo o último espaço :**

  Penso6logo@existo

- **A força da senha está no seu comprimento e em não anotá-la em papel.**

Segurança lógica

- Política de senhas do domínio



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

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

HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

Segurança lógica

- Como trocar a senha pela Intranet:

1. Acessar a intranet do TRT ;
2. Clicar no ícone de alteração de senha;
3. Preencher os campos "Informe a nova senha" e "Redigite a nova senha";
4. Clicar no botão alterar senha;

Segurança lógica

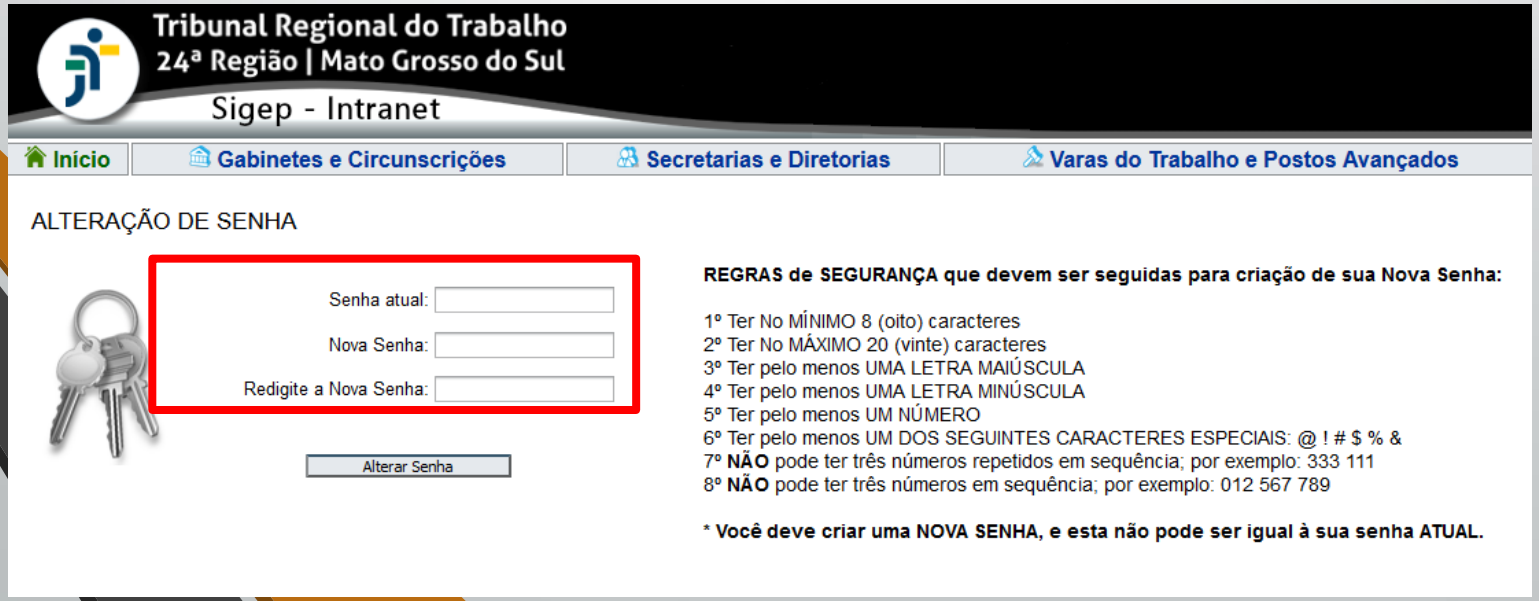
- Como trocar a senha pela Intranet:
  1. Acessar a intranet do TRT – https://intranet.trt24.jus.br ;

Segurança lógica

- Como trocar a senha pela Intranet:
  2. Clicar no ícone de alteração de senha.

Segurança lógica

- Como trocar a senha pela Intranet:
  3. Preencher os campos "Informe a nova senha" e "Redigite a nova senha";
  4. Clicar no botão alterar senha;



Segurança lógica

- Como você pode nos ajudar a melhorar a segurança das senhas ?

1. **Jamais anotá-las em papel;**
2. **Não salvar as senhas nos navegadores web (Firefox, IE) e nem no Thunderbird;**
3. **Não utilizar a mesma senha do TRT em outras plataformas (facebook, instagram, email pessoal)**

Segurança lógica

- Como você pode nos ajudar a melhorar a segurança das senhas ?

2. **Não salvar as senhas nos navegadores web (Firefox, IE) e nem no Thunderbird;**

Segurança lógica

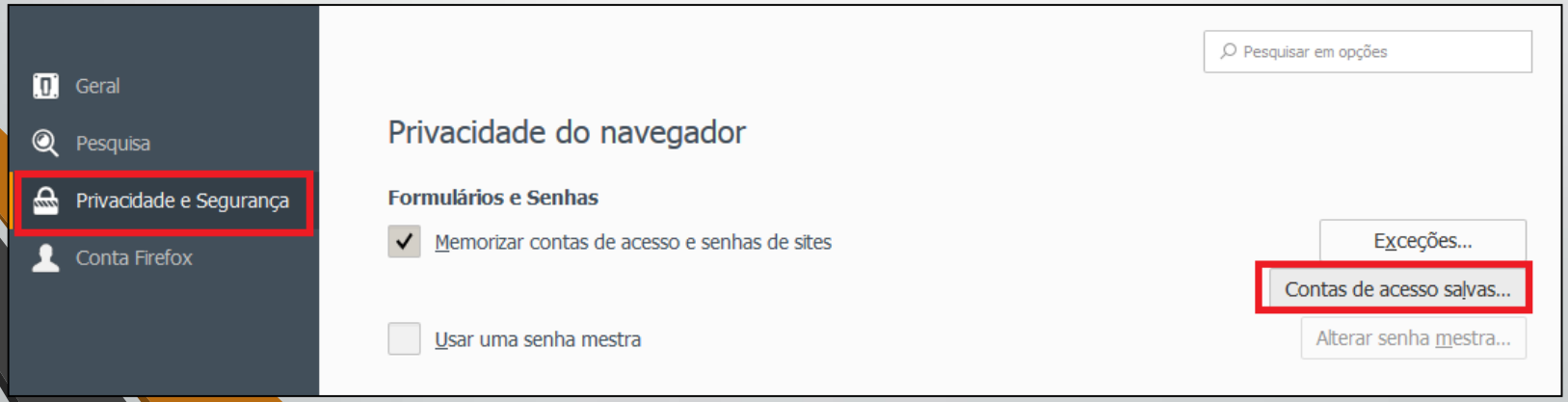
- Como você pode nos ajudar a melhorar a segurança das senhas ?

2. **Não salvar as senhas nos navegadores web (Firefox, IE) e nem no Thunderbird;**

Segurança lógica

- Como você pode nos ajudar a melhorar a segurança das senhas ?

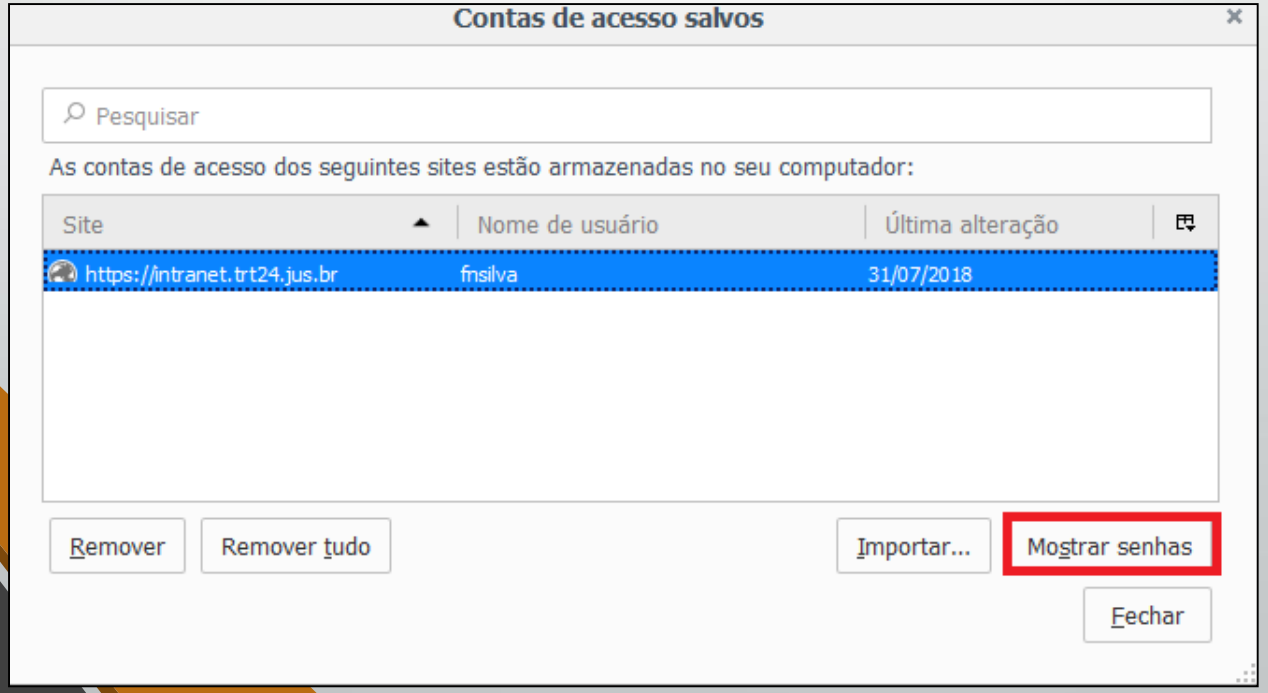
2. **Não salvar as senhas nos navegadores web (Firefox, IE) e nem no Thunderbird;**



Segurança lógica

- Como você pode nos ajudar a melhorar a segurança das senhas ?

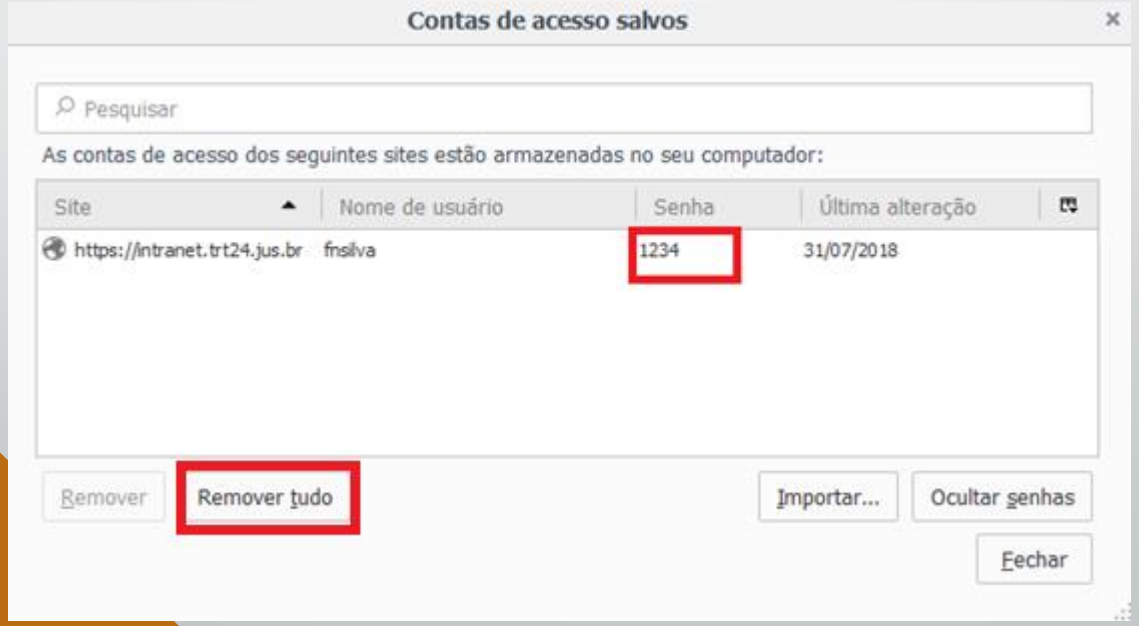
2. **Não salvar as senhas nos navegadores web (Firefox, IE) e nem no Thunderbird;**



Segurança lógica

- Como você pode nos ajudar a melhorar a segurança das senhas ?

2. **Não salvar as senhas nos navegadores web (Firefox, IE) e nem no Thunderbird;**



Segurança lógica

- Antivírus

Segurança lógica

- Antivírus - conceitos
  - **Detecção do vírus baseada em assinatura**

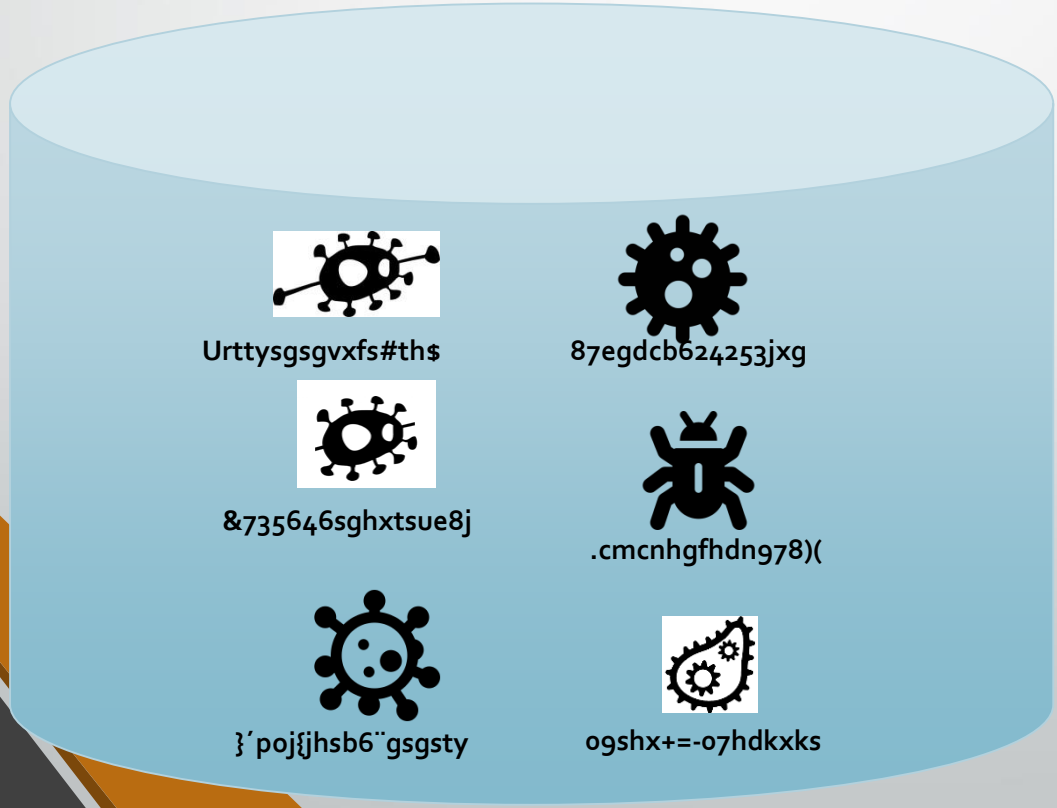
    - É como se fosse a impressão digital de um vírus. O antivírus possui um grande banco de identificadores(digitais) dos vírus conhecidos na atualidade.

  - **Detecção de vírus baseada em comportamento**

    - Vírus é identificado no sistema de acordo com os delitos que comete no sistema.

Segurança lógica

- Antivírus - conceitos
  - **Banco de dados de Assinatura de vírus:**

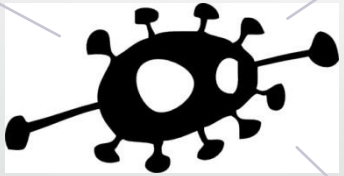


Segurança lógica

- Antivírus - conceitos
  - **Detecção de um vírus pelo comportamento**

Acesso indevido às pastas de sistema

Alterações indevidas de registros do Windows



Milhões de tentativas de conexões de rede fora do padrão

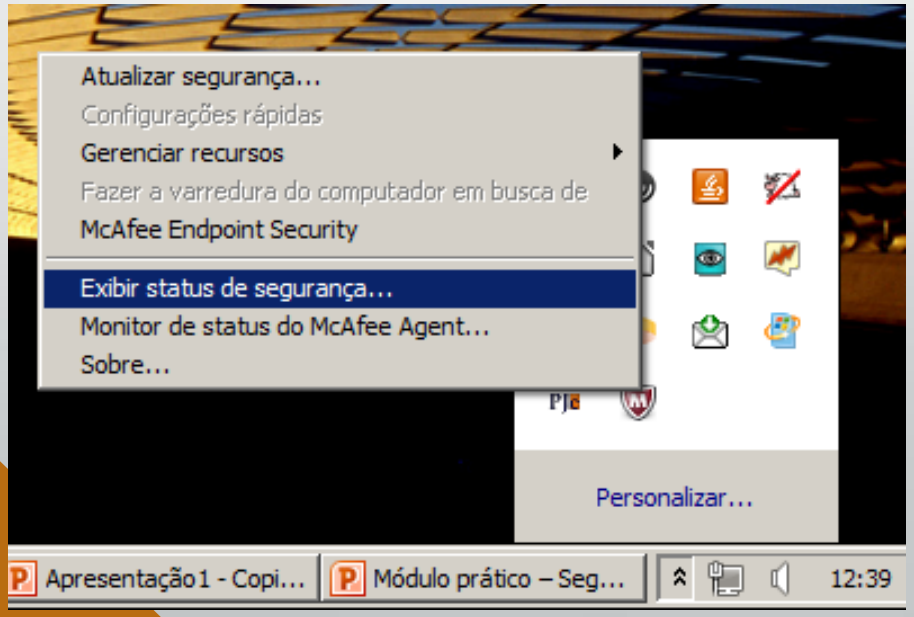
Número de acesso aos arquivos do disco fora do padrão

Segurança lógica

- Antivírus - Mcafee
  - Nosso antivírus possui proteção baseada em assinatura e comportamento.
  - A atualização da base de assinaturas é automática, mas devemos estar atento para possíveis problemas nesse processo.

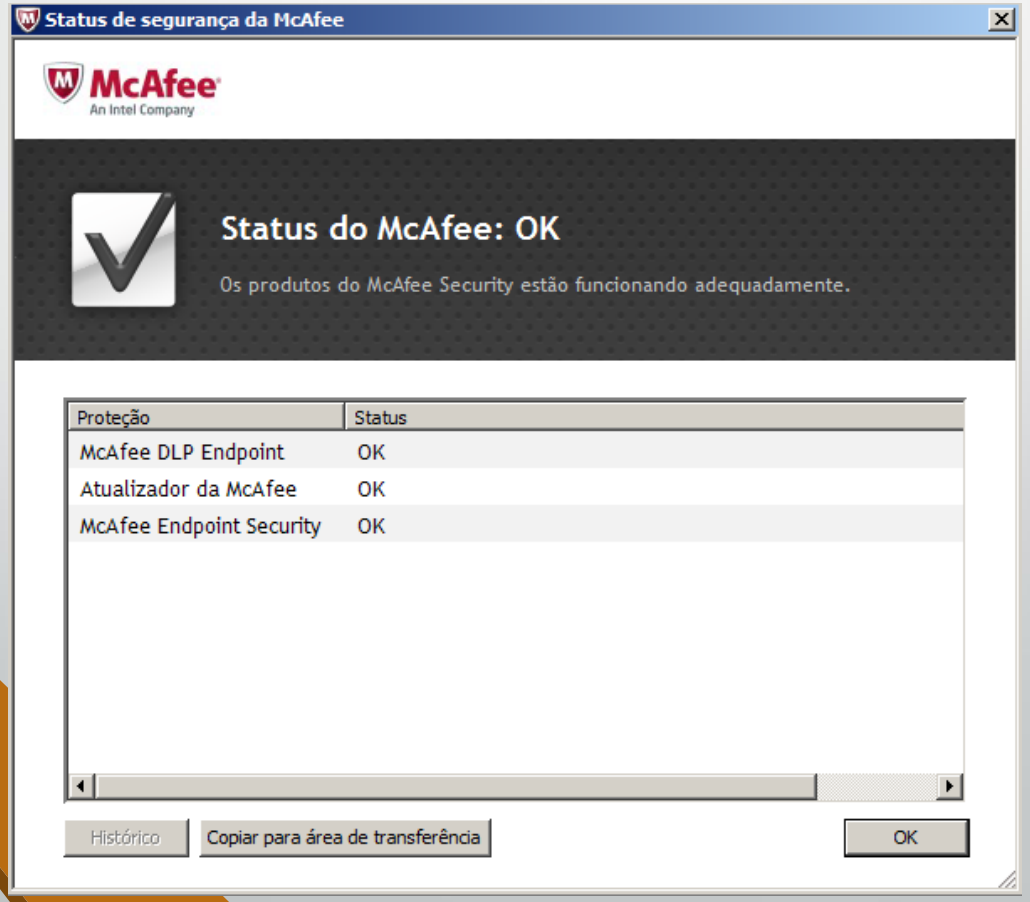
Segurança lógica

- Como você pode nos ajudar a melhorar a segurança no antivírus ?
  - **Verifique se você está protegido;**
  1. **Abra a barra de tarefas do Windows**
  2. **Clique com o botão direito do mouse no ícone**
  3. **Clique na opção "Exibir status de segurança"**



Segurança lógica

- Como você pode nos ajudar a melhorar a segurança no antivírus ?



Segurança lógica

- Política da mesa limpa

Segurança lógica

- Política da mesa limpa
  - **Informações confidenciais não devem ser anotadas em papel e deixadas sobre a mesa.**
  - **Bloquear ou desligar o computador ao se ausentar da sala, mesmo que temporariamente.**

    Dica: teclas "⊞ + L" bloqueiam a estação.
  - **Documentos confidenciais devem ser trancados em armário ou gaveta apropriado.**
  - **Não comer ou beber próximo aos computadores.**

Segurança lógica

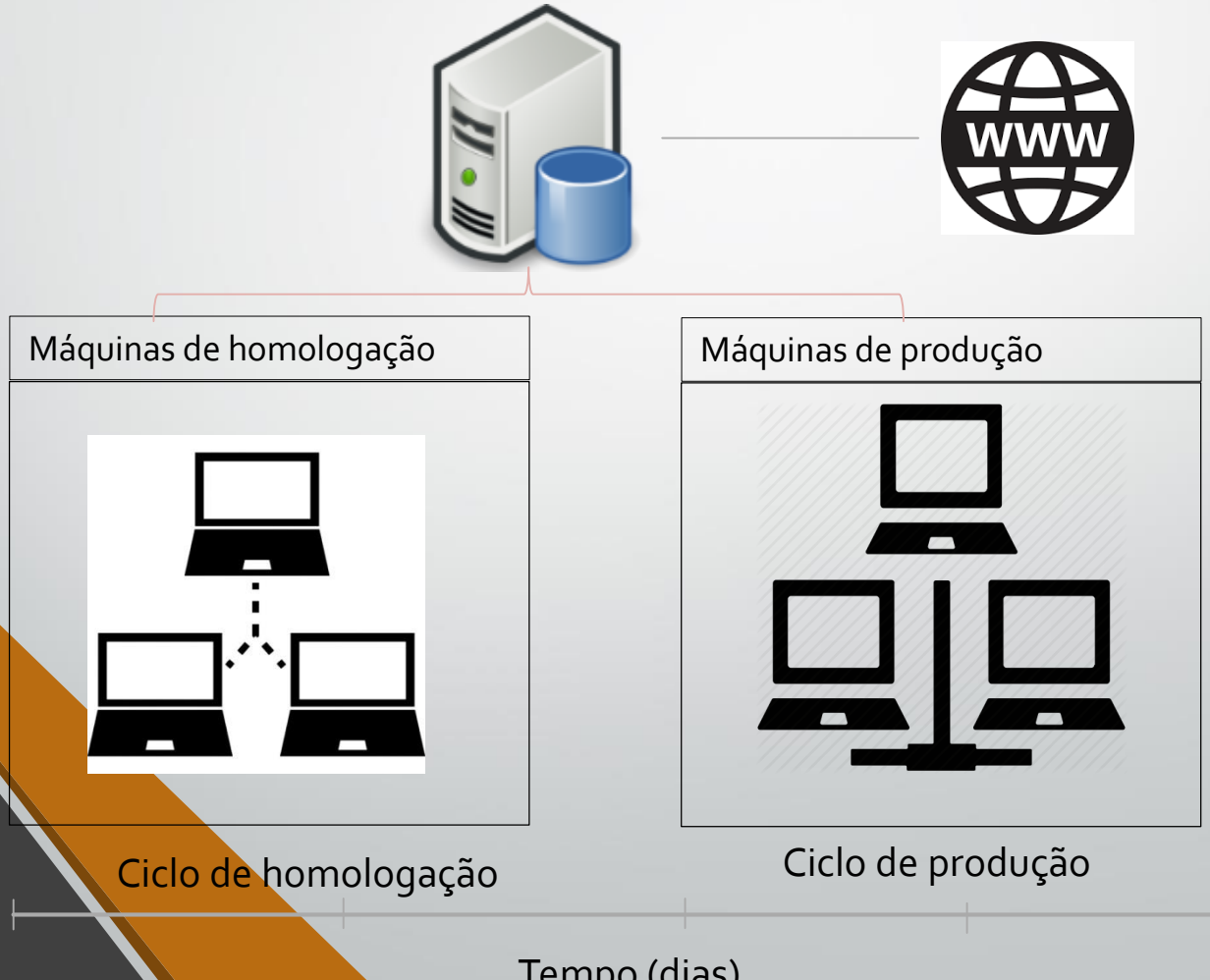
- Windows update

Segurança lógica

- Windows update
  - **As atualizações são desenvolvidas pela Microsoft para resolver fraquezas de segurança encontradas pelos Hackers ao longo do tempo no Windows.**
  - **Sistemas desatualizados estão muito mais suscetíveis a ataques.**
  - **Ransowares se proliferam devido a falta de atualização dos sistemas operacionais (Windows).**
  - **Não só Windows desatualizado, mas outros aplicativos podem ser portas de entrada para softwares maliciosos (aplicativos utilitário, sistemas internos com contraindicação para utilização externa, etc)**

Segurança lógica

- Windows update



Segurança lógica

- Principais ataques aos computadores

Segurança lógica

- Principais ataques aos computadores

1. **Engenharia social;**
2. **Quebra de confidencialidade em redes sem fio;**
3. **Ransoware**

Segurança lógica

- Principais ataques aos computadores

1. **Engenharia social: arte de manipular as pessoas a fim de contornar os mecanismos e dispositivos de segurança.**

Segurança lógica

- Principais ataques aos computadores

1. **Engenharia social – como você pode ajudar?**

   - **Não exponha informações pessoais nas redes sociais;**
   - **Jamais passe informações confidenciais por telefone;**
   - **Antes de passar seu IP para nossos técnicos da SETIC, tenha certeza de que realmente são eles (reconhecimento de voz, ramal, informações que ele deveria saber, número do SIATE);**
   - **Acompanhe o acesso remoto até o fim;**
   - **Desconfie de e-mails com promoções espetaculares ou que solicitem informações pessoais como senhas, cpf, etc.**

Segurança lógica

- Principais ataques aos computadores

2. **Quebra de confidencialidade em redes sem fio**

Segurança lógica

- Principais ataques aos computadores

2. **Quebra de confidencialidade em redes sem fio – como você pode ajudar?**

    - **Mantenha o sistema operacional do seu computador atualizado;**
    - **Não acesse redes sem fio públicas a partir do seu celular, principalmente se for utilizar senhas e internet banking;**
    - **Acessar apenas sites com criptografia (https://);**
    - **Se possível, sempre prefira redes cabeadas a redes sem fio.**

Segurança lógica

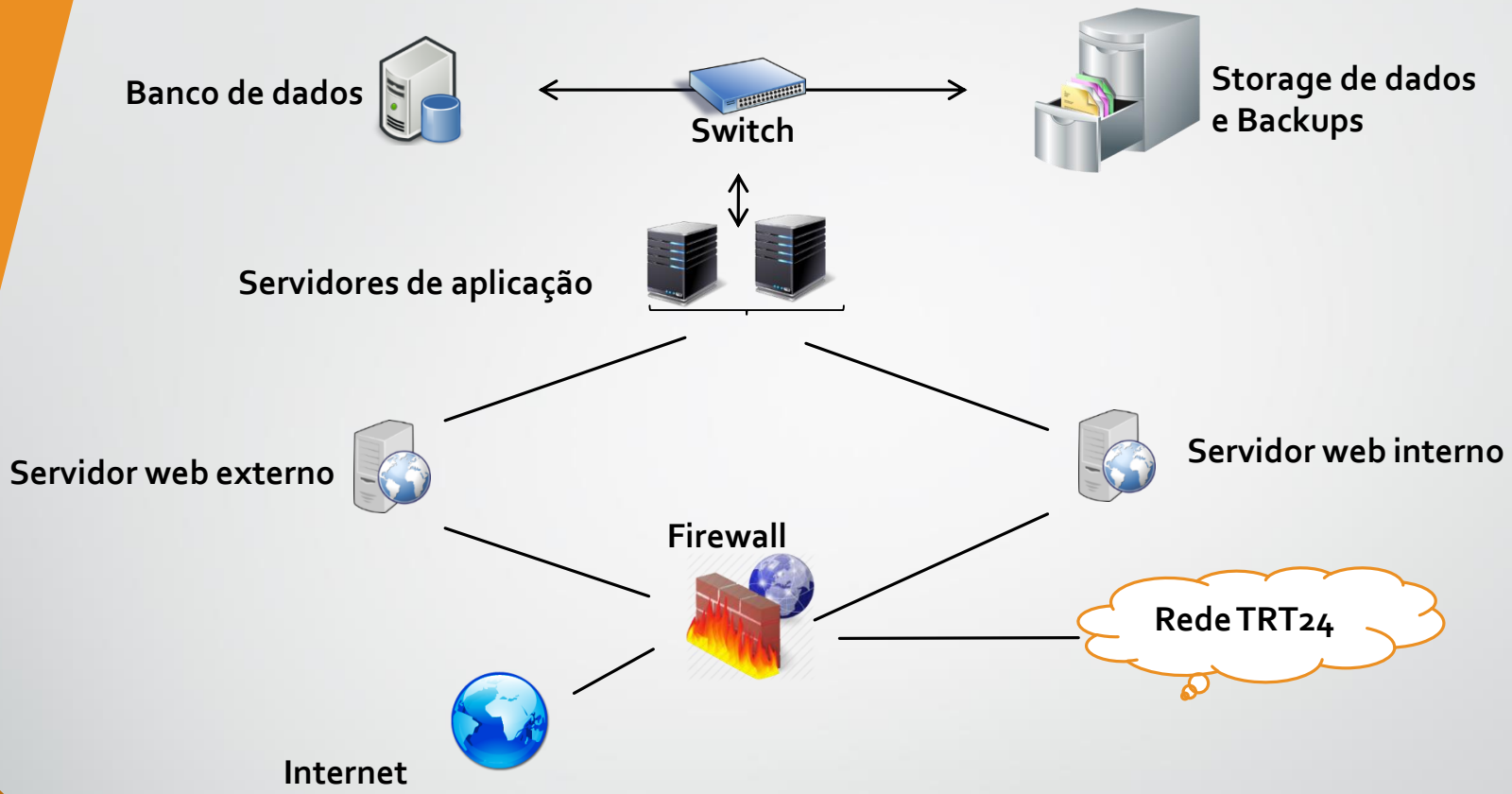
- Principais ataques aos computadores

3. **Ransoware – sequestro de informação**

Ransoware – contaminação

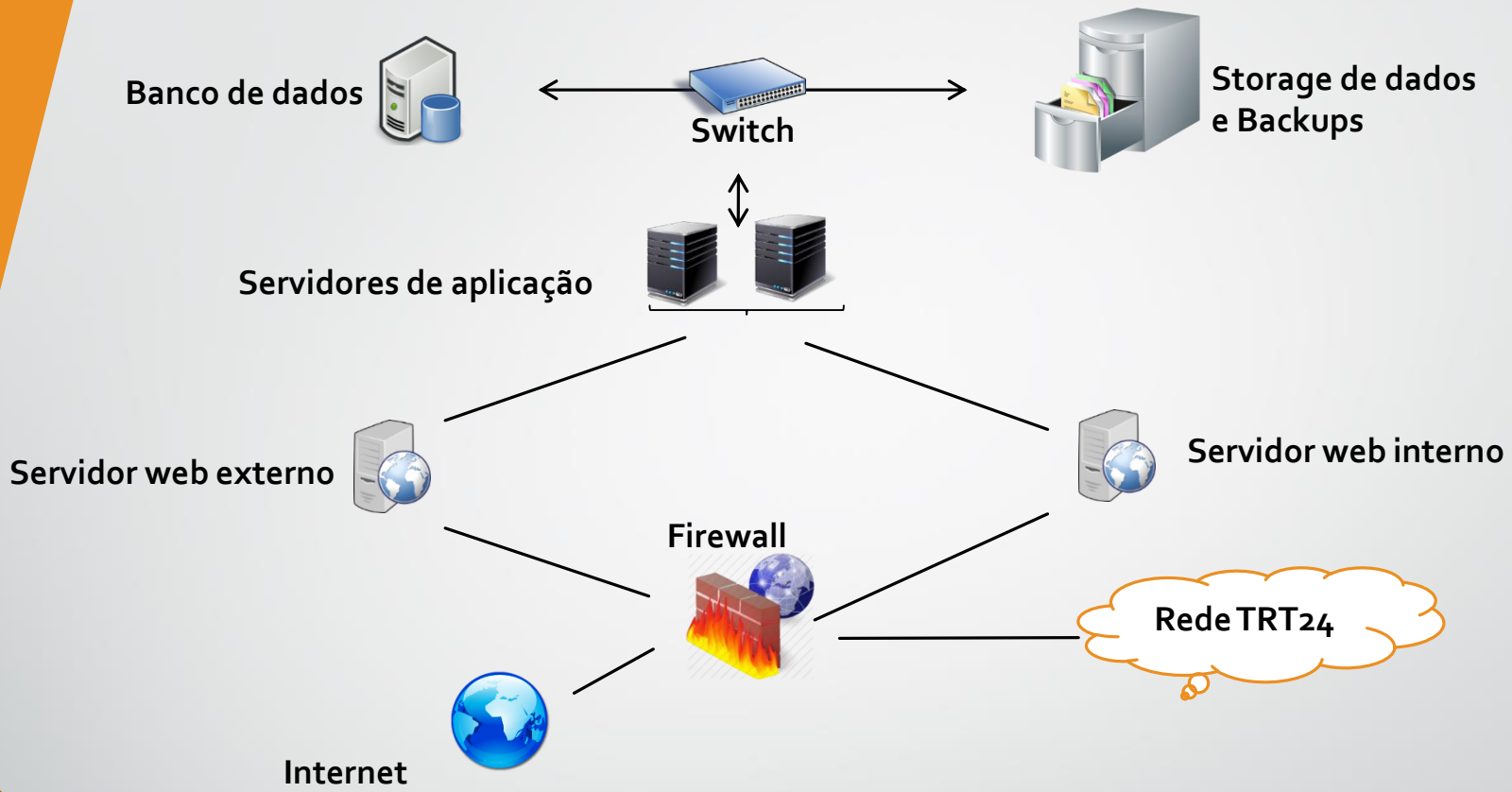
Ransoware – contaminação

Ransoware – contaminação



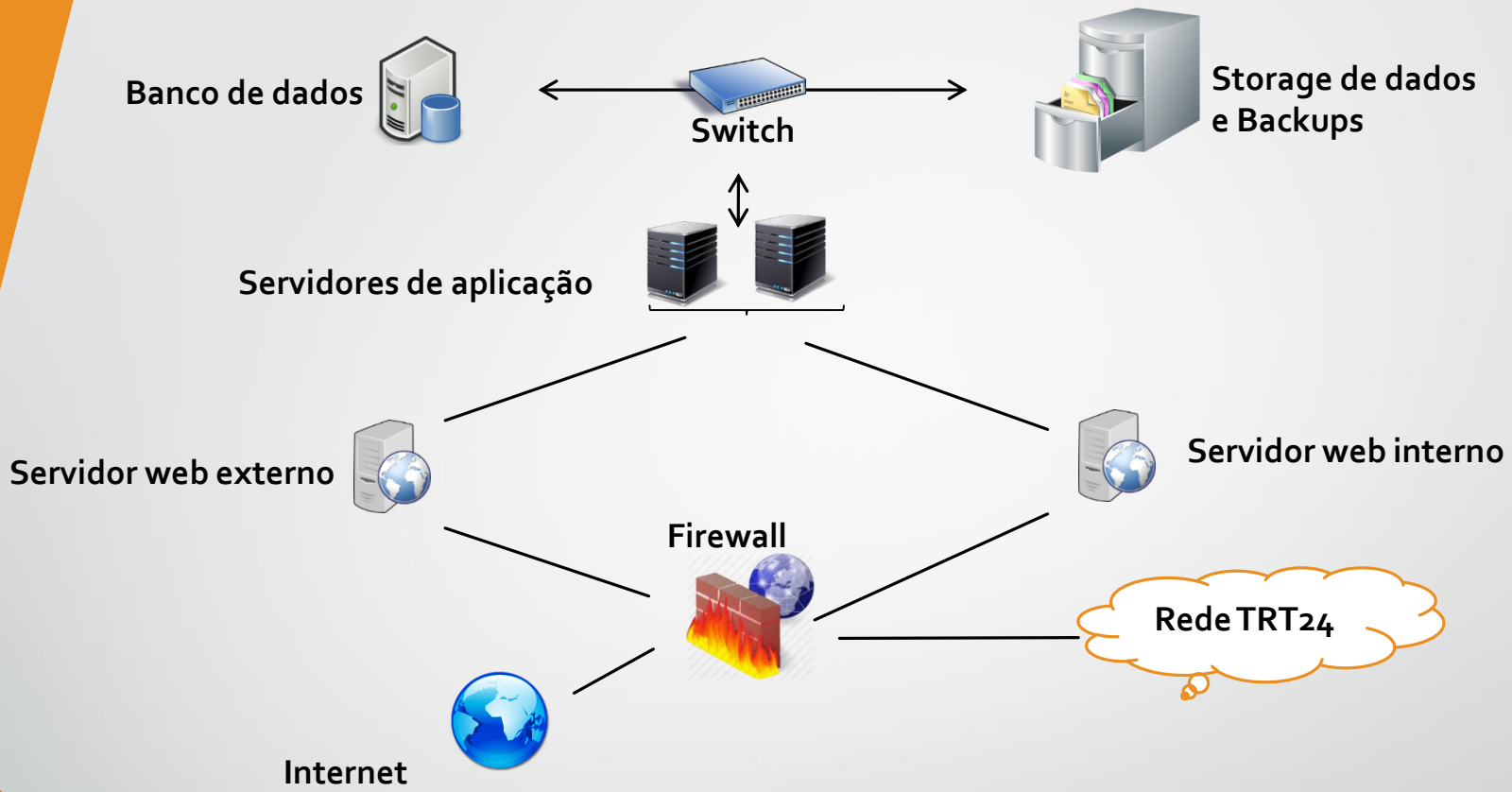
NÃO VERIFICAR SE ANTIVÍRUS E WINDOWS ESTÃO COM AS ÚLTIMAS ATUALIZAÇÕES

Ransoware – contaminação



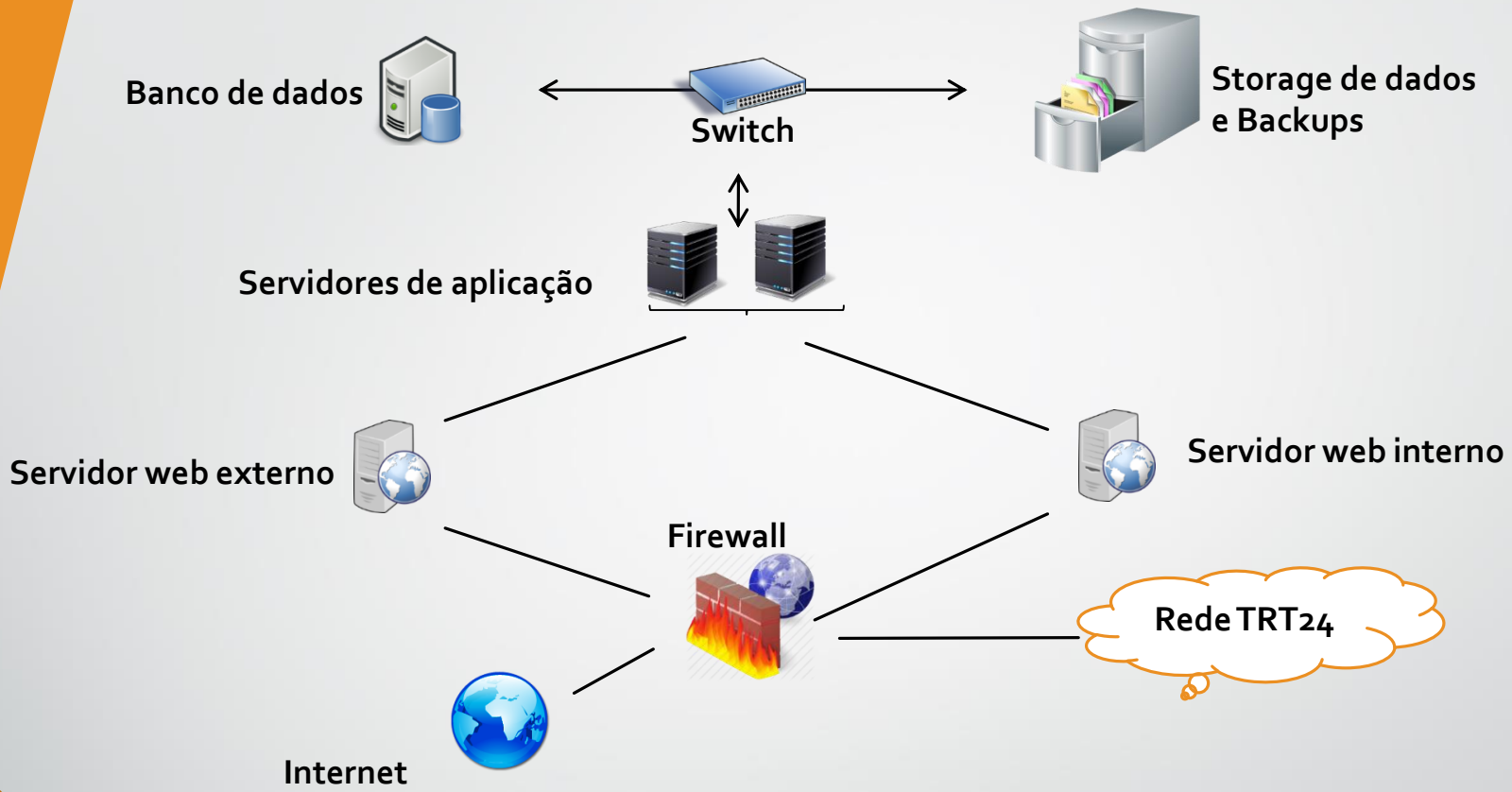
CLICAR EM LINKS E ANEXOS DE EMAILS CONTAMINADOS

Ransoware – contaminação



BAIXAR E EXECUTAR ARQUIVOS CONTAMINADOS DE SITES INSEGUROS

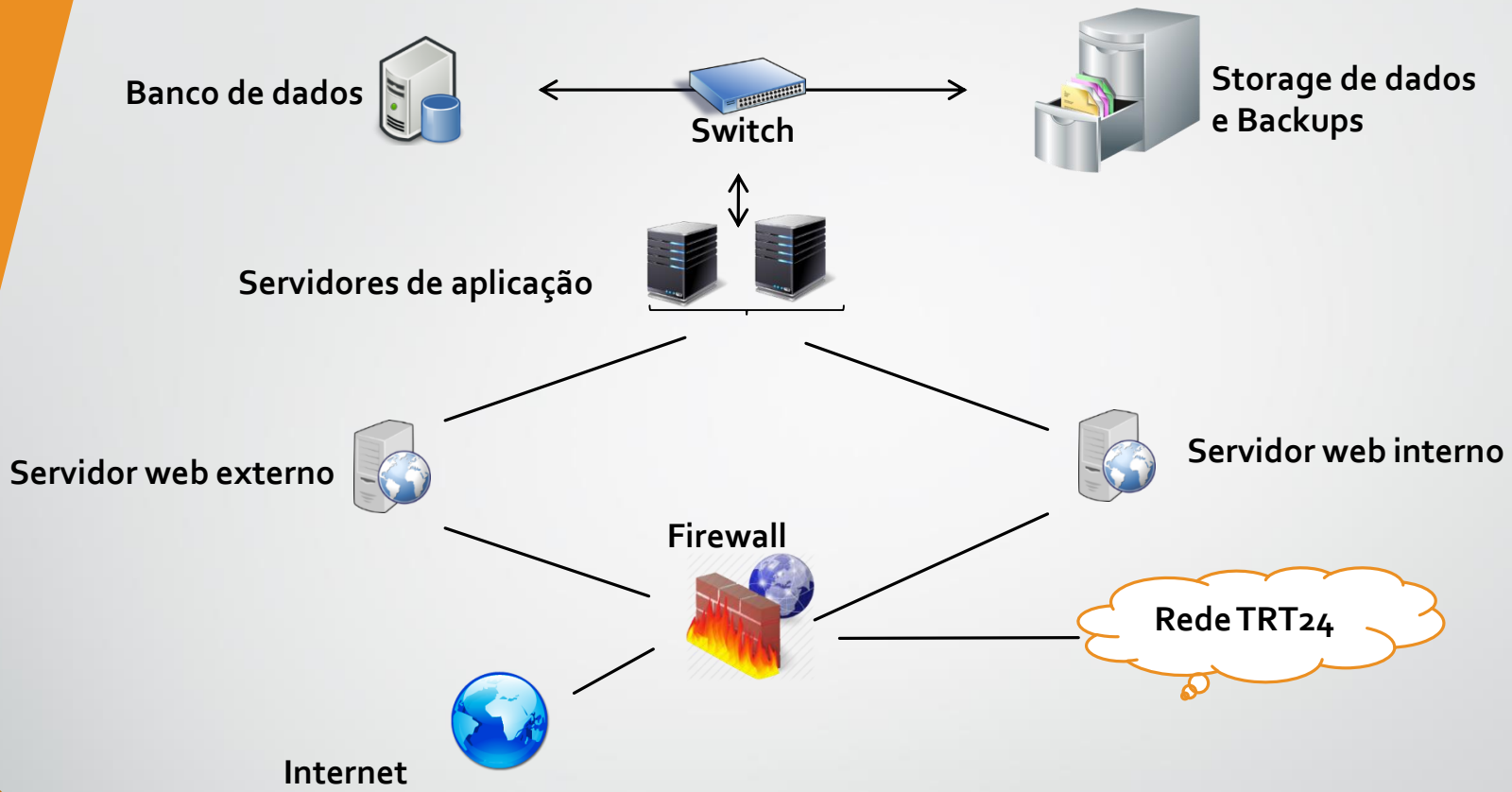
Ransoware – contaminação



INSTALAR SOFTWARES SEM O ACOMPANHAMENTO DA TI

VOCÊ

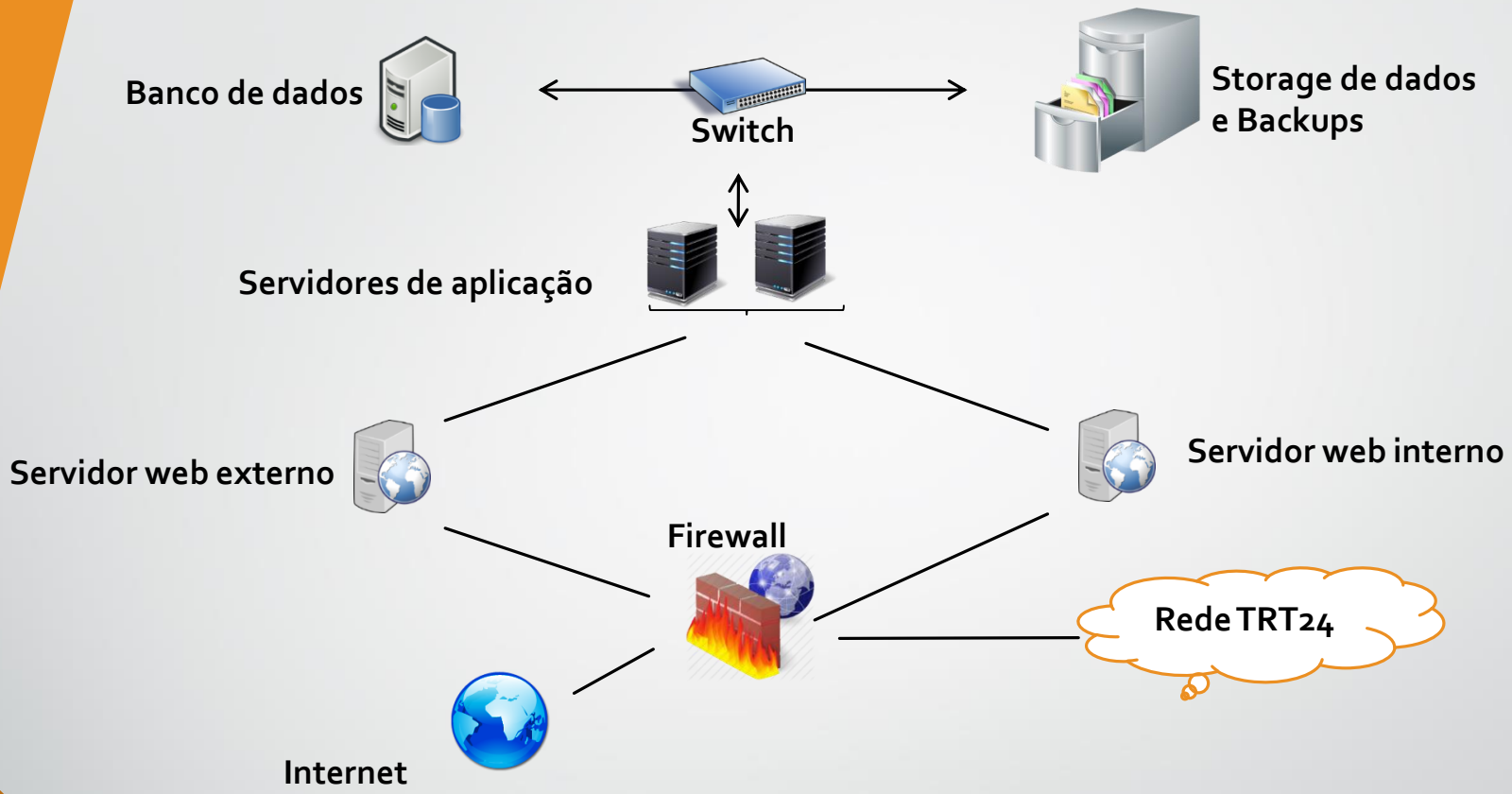
Ransoware – contaminação



DESATIVAR O ANTIVÍRUS POR CONTA PRÓPRIA

VOCÊ

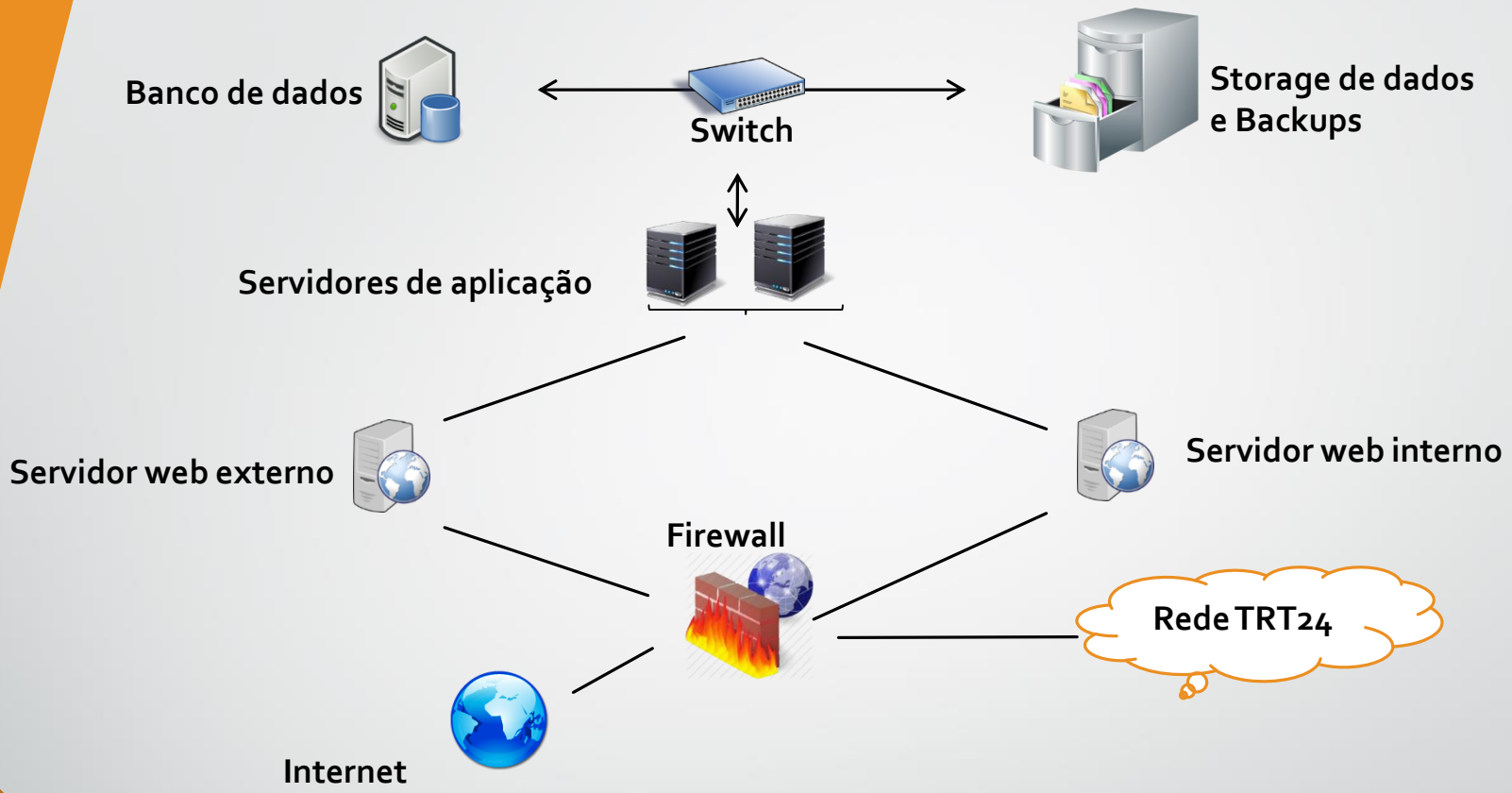
Ransoware – contaminação



NÃO UTILIZAR SENHAS FORTES PARA O SEU LOGIN

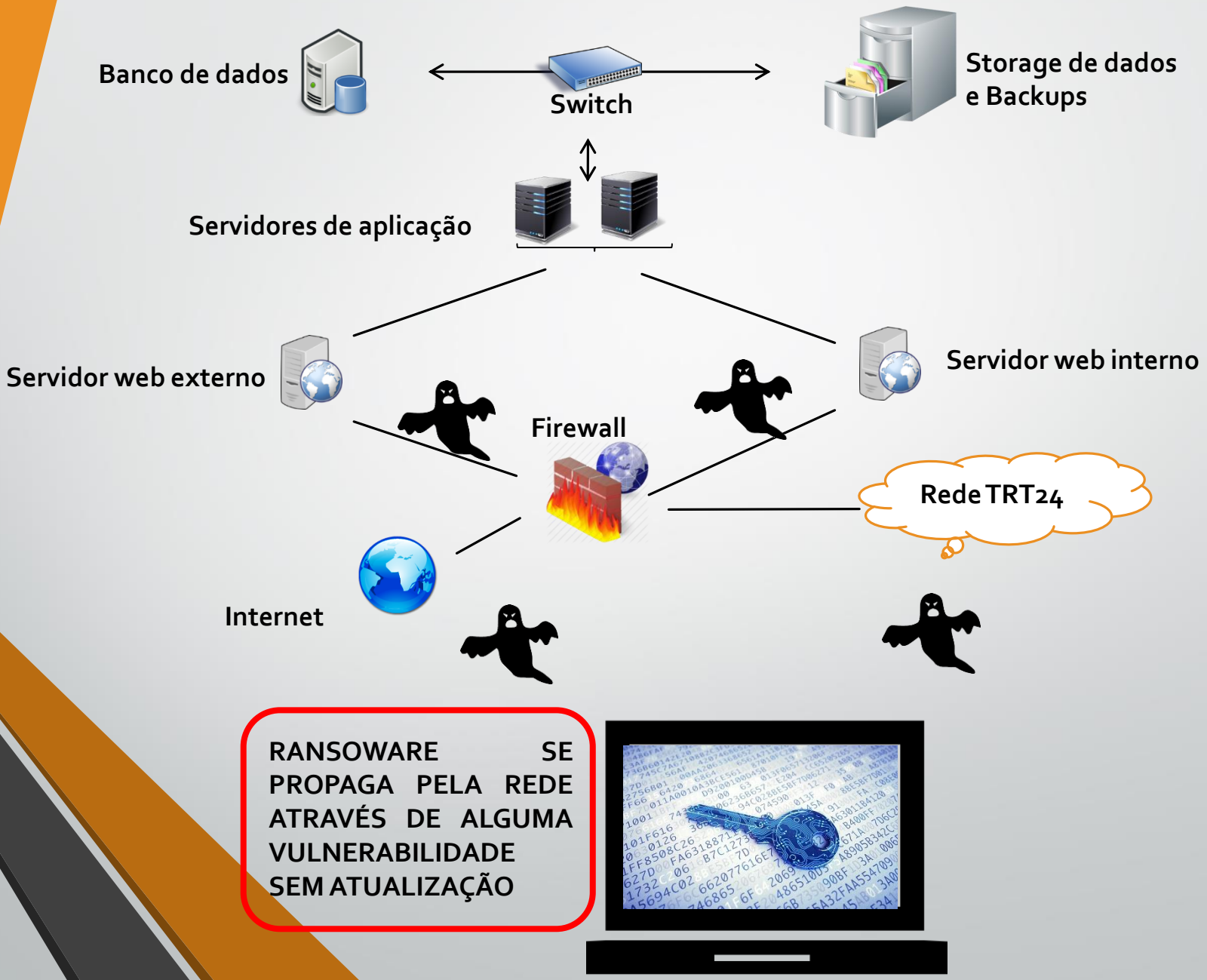
VOCÊ

Ransoware – contaminação



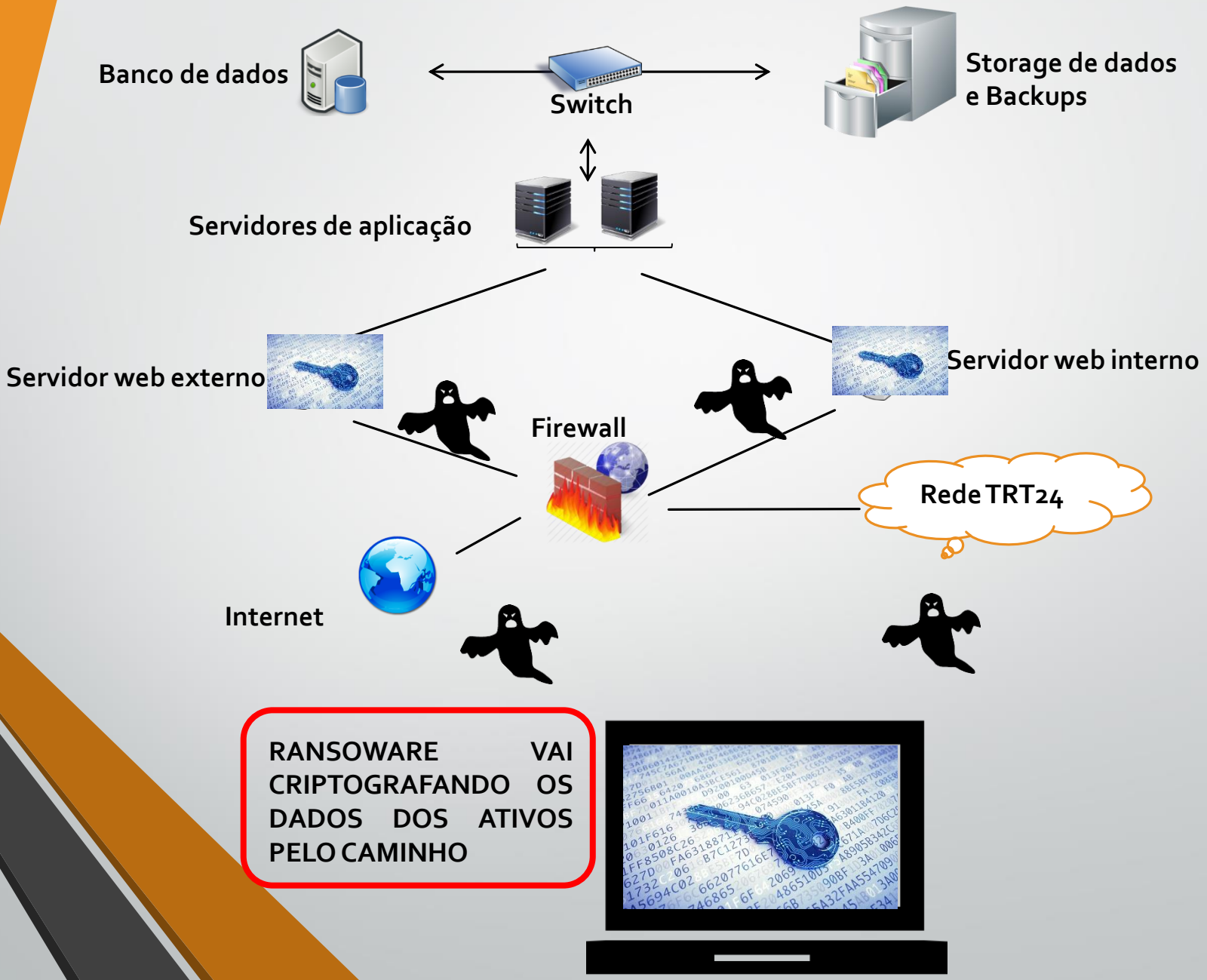
RANSOWARE CRIPTOGRAFA DADOS LOCAIS DA SUA ESTAÇÃO

Ransoware – contaminação

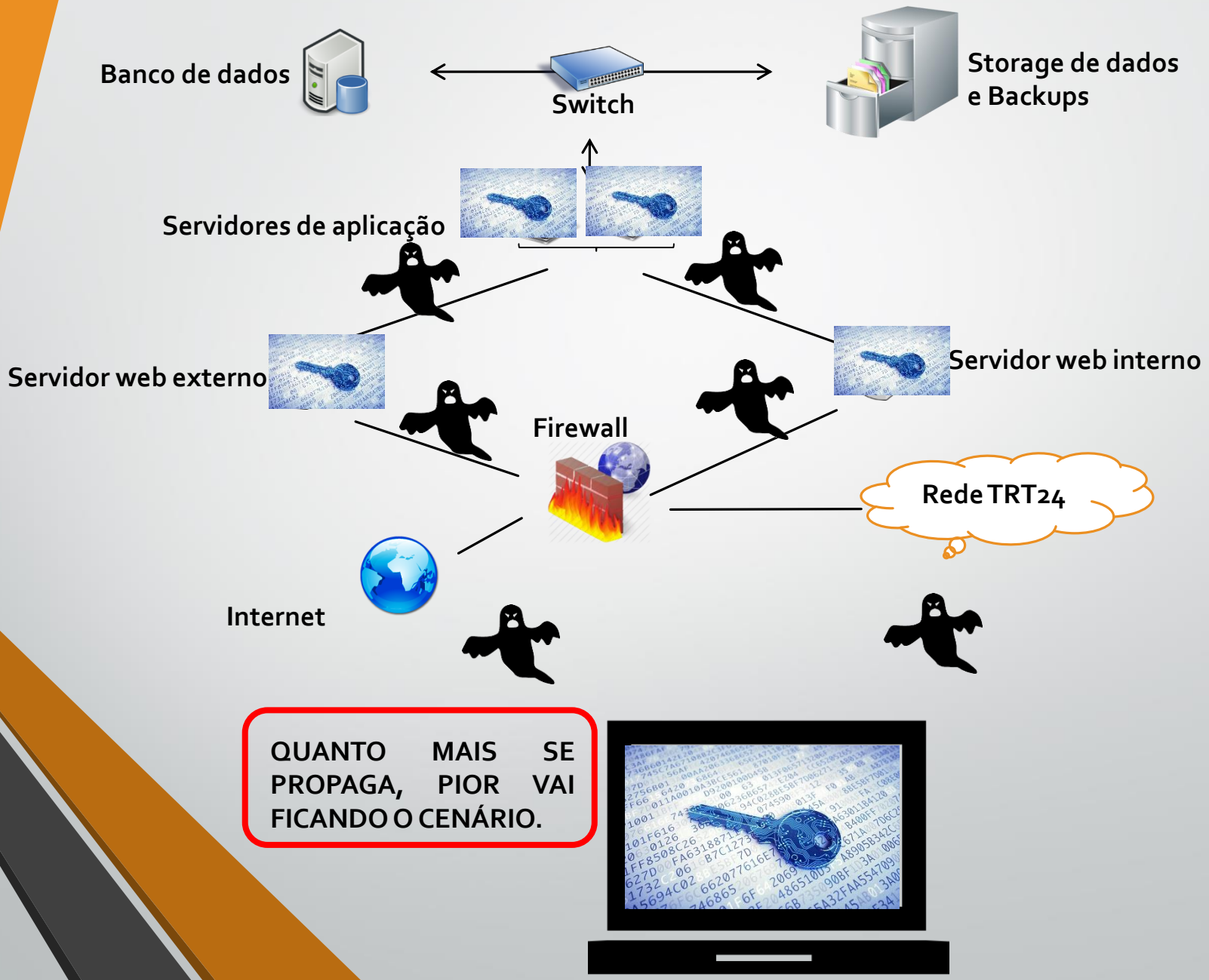


RANSOWARE SE PROPAGA PELA REDE ATRAVÉS DE ALGUMA VULNERABILIDADE SEM ATUALIZAÇÃO

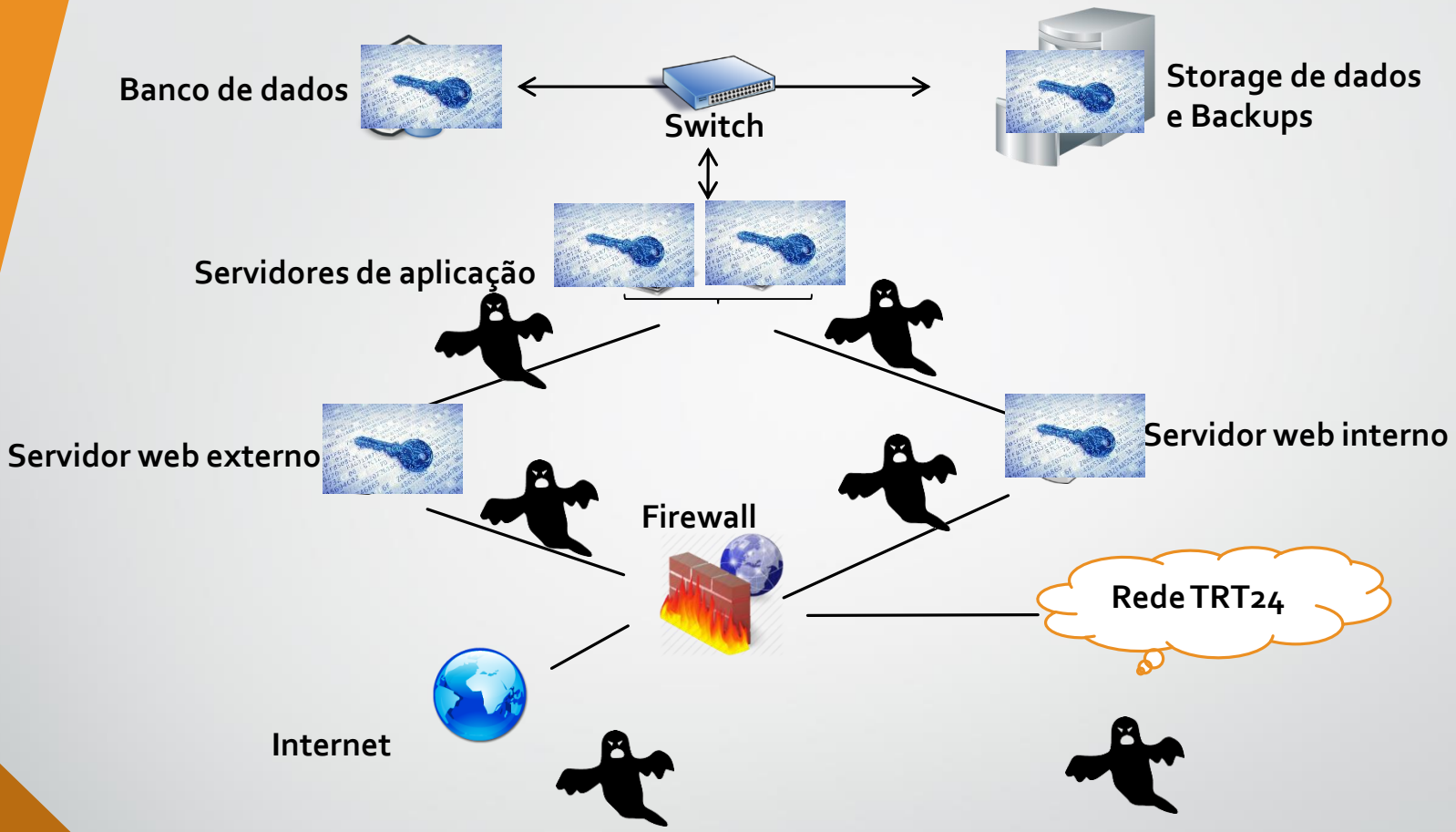
Ransoware – contaminação



Ransoware – contaminação

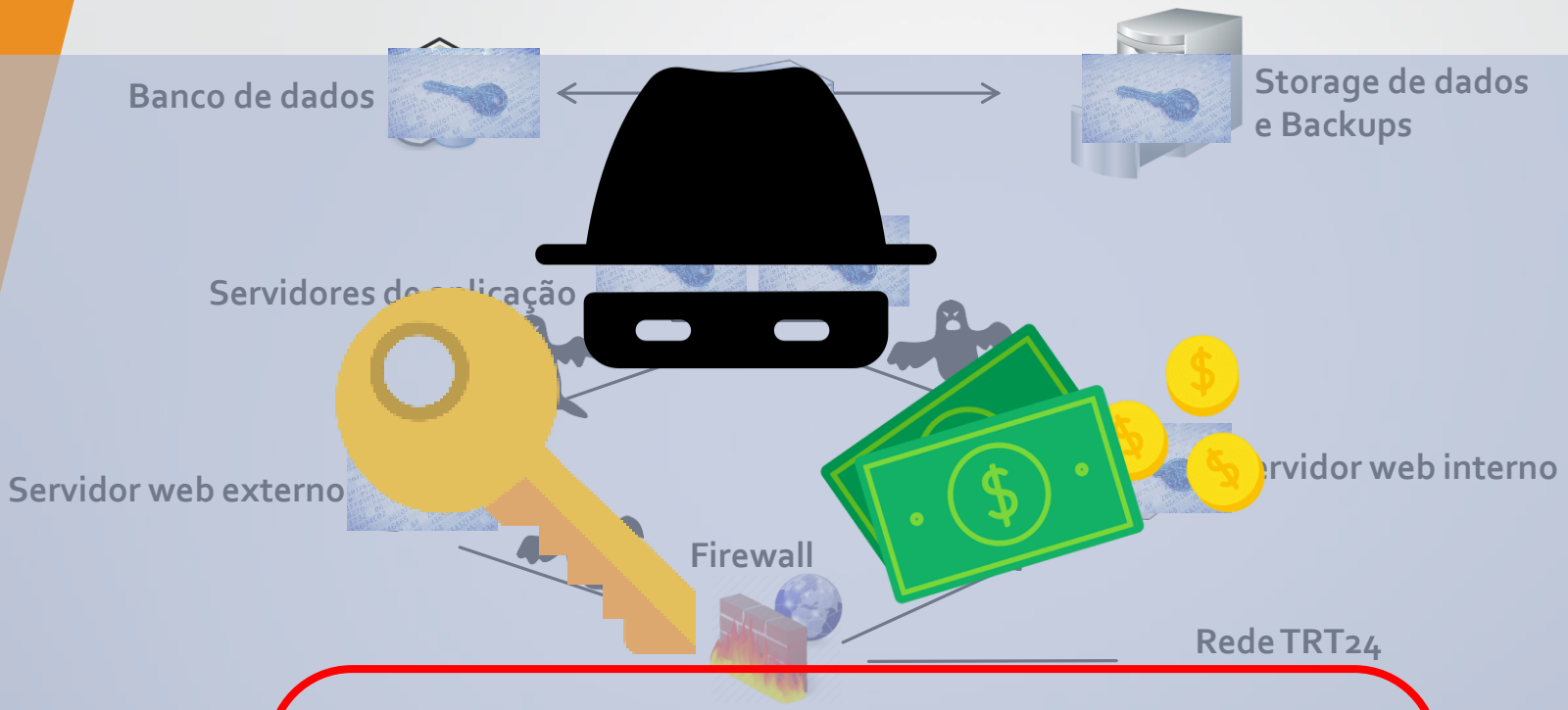


Ransoware – contaminação



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

Ransoware – contaminação



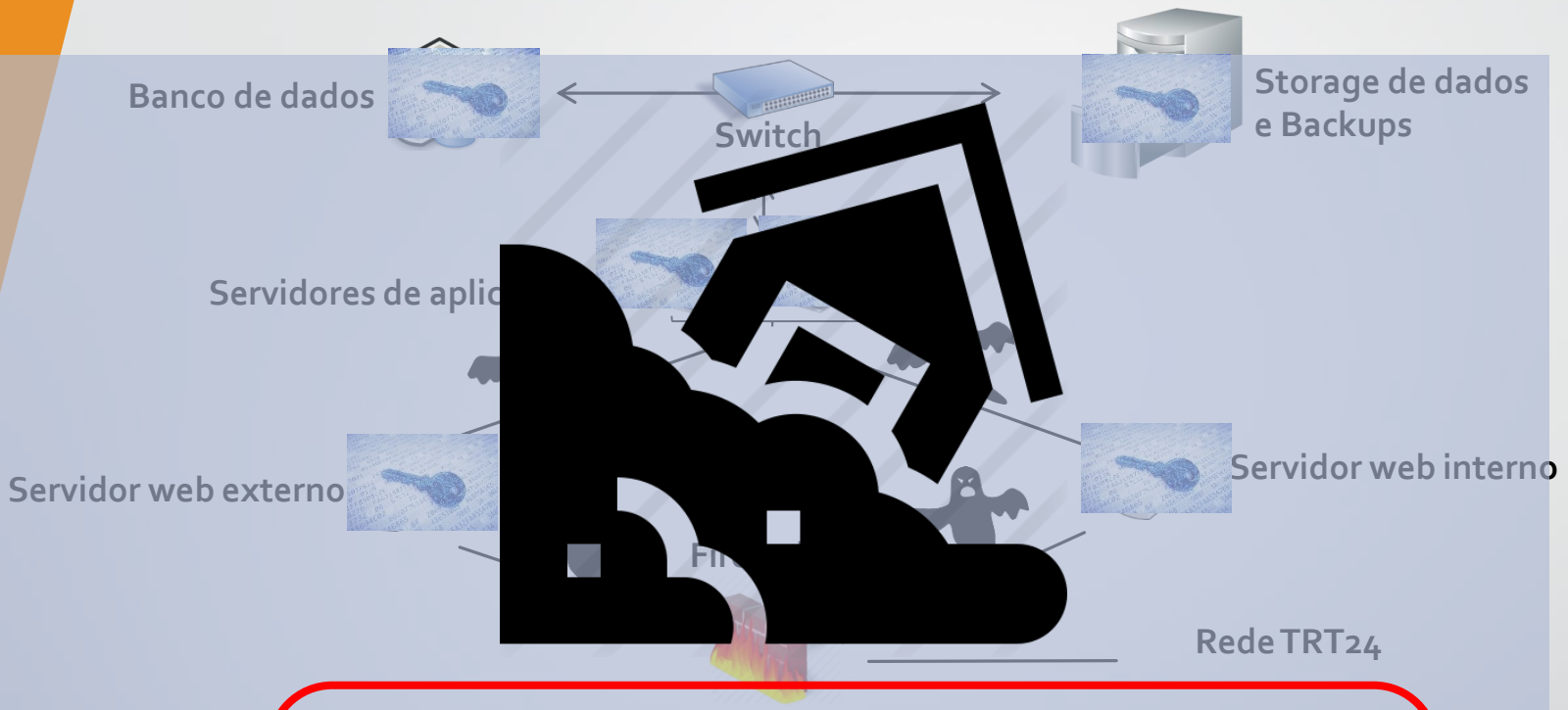
-NO FINAL DE TUDO, O ATACANTE PEDE RESGATE EM TROCA DA CHAVE CAPAZ DE RECUPERAR AS INFORMAÇÕES.

-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.

Semana da Segurança da Informação

- Do dia 24/05 a 28/05, foram definidas uma série de ações EMERGENCIAIS para respondermos a recente onda de ataques cibernéticos às instituições públicas.
- Precisamos da ajuda de TODOS nessa corrente da Segurança. Não seja o ELO FRACO desse esforço.

Semana da Segurança da Informação - Ações

- Ações técnicas da SETIC
- Ações individuais, relacionada aos colaboradores do TRT24.

Semana da Segurança da Informação – Ações técnicas SETIC

1. Disponibilizar últimas atualizações do antivírus e Windows
2. Aumentar segmentação das redes de dados
3. Desativar o gerenciamento do antivírus "sem senha"
4. Atualização dos serviços de acesso remoto externo(teletrabalho) e DNS
5. Varredura de vulnerabilidades nos serviços do TRT24

Semana da Segurança da Informação – Ações individuais

1. Verificar o status de funcionamento do seu antivírus.
2. Atualizar o Windows no seu computador.
3. Evitar acesso indevido de terceiros aos equipamentos e instalações do TRT24.
4. Atualizar a política de antivírus do seu notebook ou computador institucional FORA da rede de dados do TRT24.
5. Trocar sua senha na Intranet.
6. Não utilizar mais usuários genéricos e compartilháveis.
7. Acesso remoto a sua estação deverá ser autorizado e acompanhado em tempo integral por você.
8. O gabinete virtual antigo será DESATIVADO.

Semana da Segurança da Informação – Ações individuais

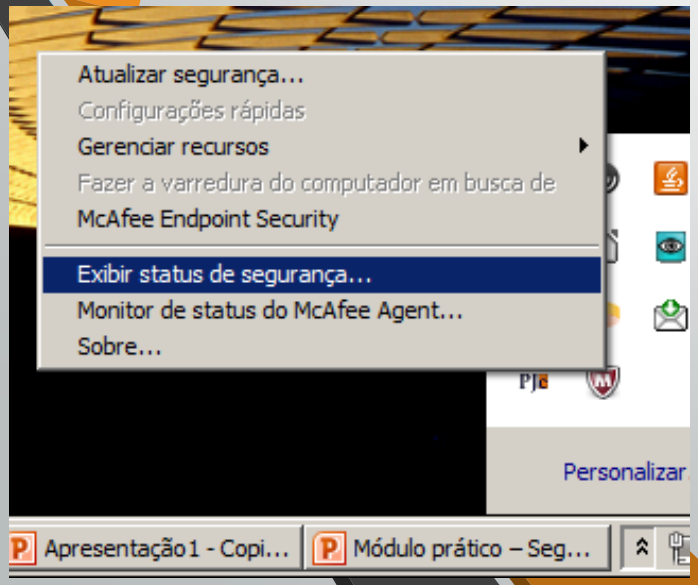
1. Verificar o status de funcionamento do seu antivírus 
   - Em caso de mau funcionamento, abra um SIATE para verificação.

Semana da Segurança da Informação – Ações individuais

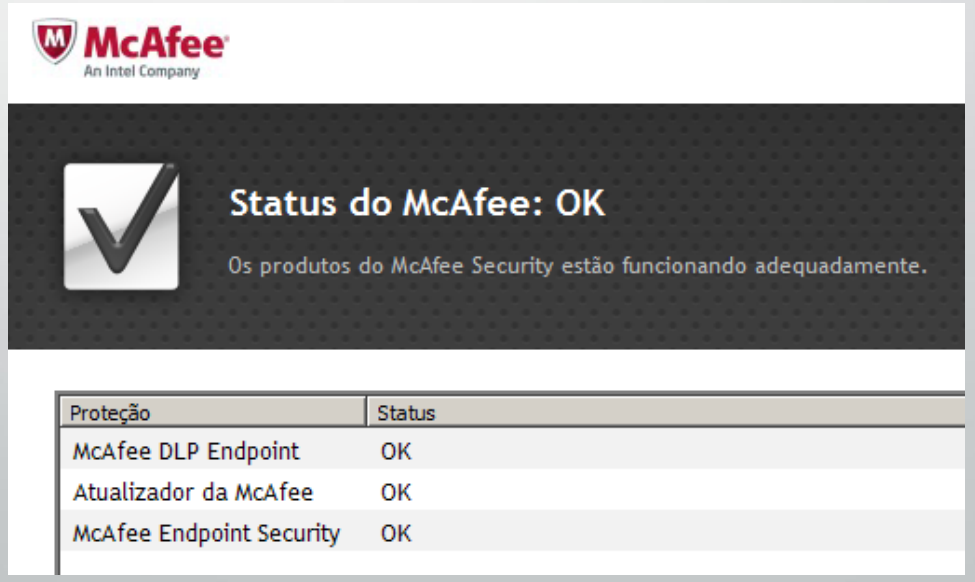
1. Verificar o status de funcionamento do seu antivírus

- Relembrando ...

1. Clicar na barra de tarefas do Windows



2. No ícone do antivírus , clicar em "Exibir status de segurança"



Semana da Segurança da Informação – Ações individuais

2. Atualizar o Windows no seu computador 
   - Devido ao trabalho remoto, máquinas estão a bastante tempo sem atualizações.
   - Se o computador que você utiliza está **FORA** da rede do TRT:
     - **Abra SIATE** para que nossa equipe configure as atualização pela Internet
   - Se o computador que você utiliza está **DENTRO** da rede do TRT:
     - Apenas deixe **LIGADO** o computador para que possa ser atualizado adequadamente.

Semana da Segurança da Informação – Ações individuais

2. Atualizar o Windows no seu computador – possíveis problemas:
   - Pior caso:
     - Atualizações causarem mau funcionamento do computador que impeçam a manutenção remota por nossa equipe.
     - Nesses casos raros, a única solução seria agendar o transporte da máquina até o TRT para solução.
   - Mas lembre-se: os riscos e problemas ocasionados por um computador desatualizado são muito PIORES:
     - Possíveis danos irreparáveis à imagem da instituição.
     - Roubo de dados e informações sensíveis.
     - Extorsão para resgate de informações criptografadas

Semana da Segurança da Informação – Ações individuais

3. Evitar acesso indevido de terceiros aos equipamentos e instalações do TRT24

- Política da mesa limpa
  - Bloquear o computador ao sair.
  - Não permitir que outros utilizem o seu login.

- Segurança física
  - Atenção a pessoas estranhas ao ambiente e sem crachá.
  - Acompanhar acesso de terceiros autorizados aos perímetros críticos.

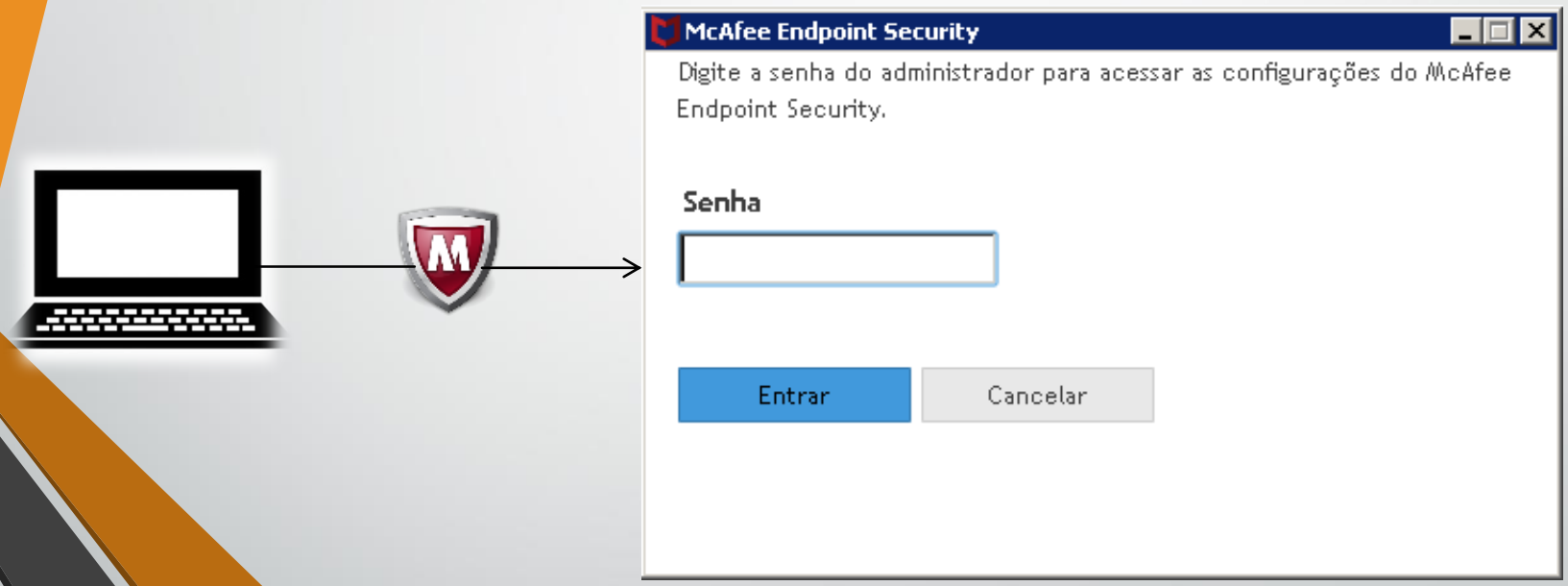
Semana da Segurança da Informação – Ações individuais

4. Atualizar a política de SENHAS do antivírus do seu notebook ou estação FORA da rede de dados do TRT24

- Abrir SIATE para atualização da política de senhas do antivírus.
- A partir de agora, não será mais possível desabilitar o antivírus sem conhecer a senha do administrador.

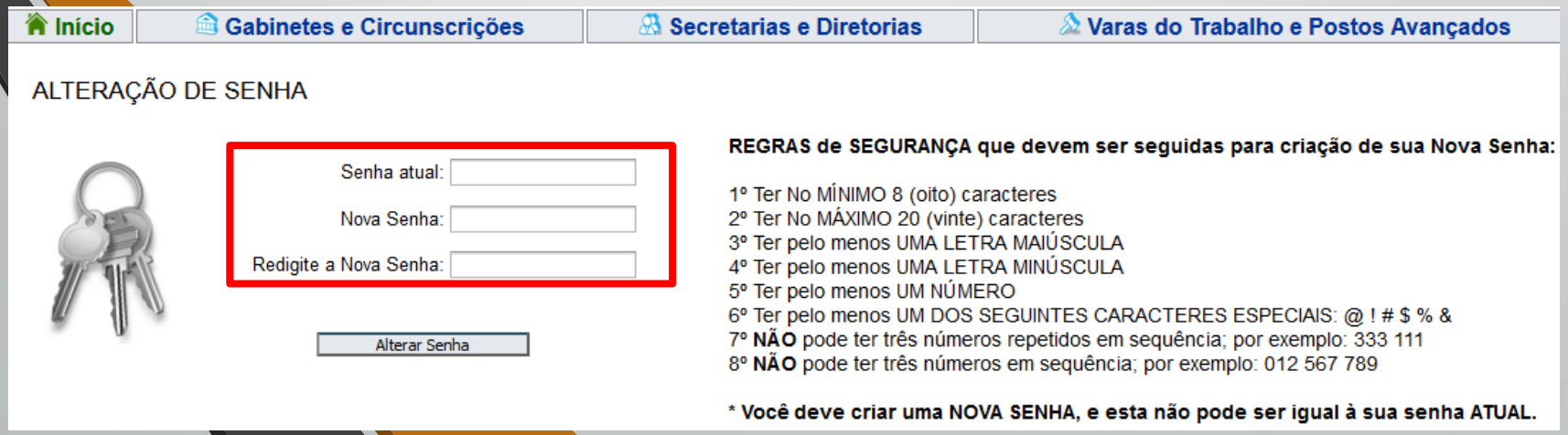
Semana da Segurança da Informação – Ações individuais

4. Atualizar a política de antivírus do seu notebook



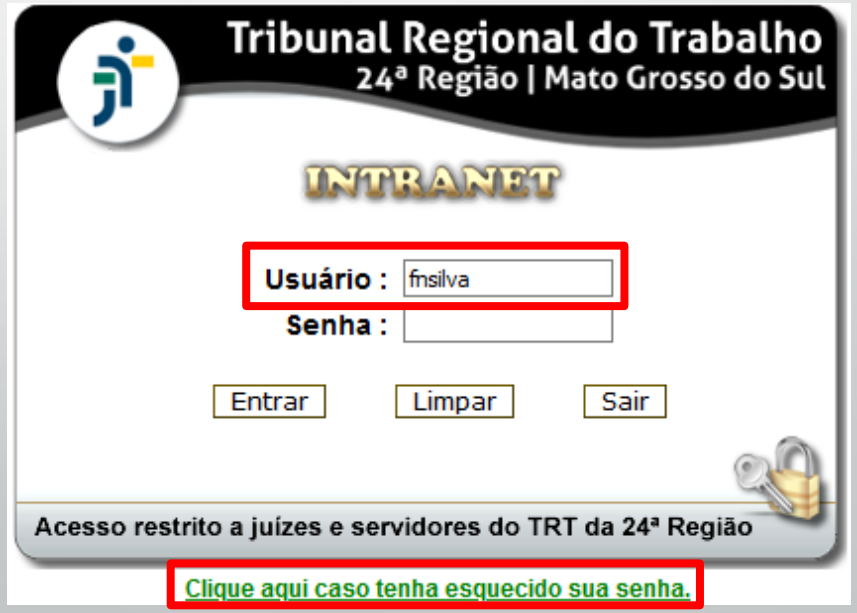
Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet
   - Os usuários que não trocarem a sua senha no período de 24/05 a 28/05, terão todos os seus acessos suspensos. **Não deixe para a última hora.**
     - Exceção: quem já trocou a sua senha na Intranet nos últimos 90 dias.
   - **Relembrando:** para trocar a senha, acesse https://intranet.trt24.jus.br/intra-vwp/faces/alteraSenha.jsp



Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha no período solicitado
        - 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.

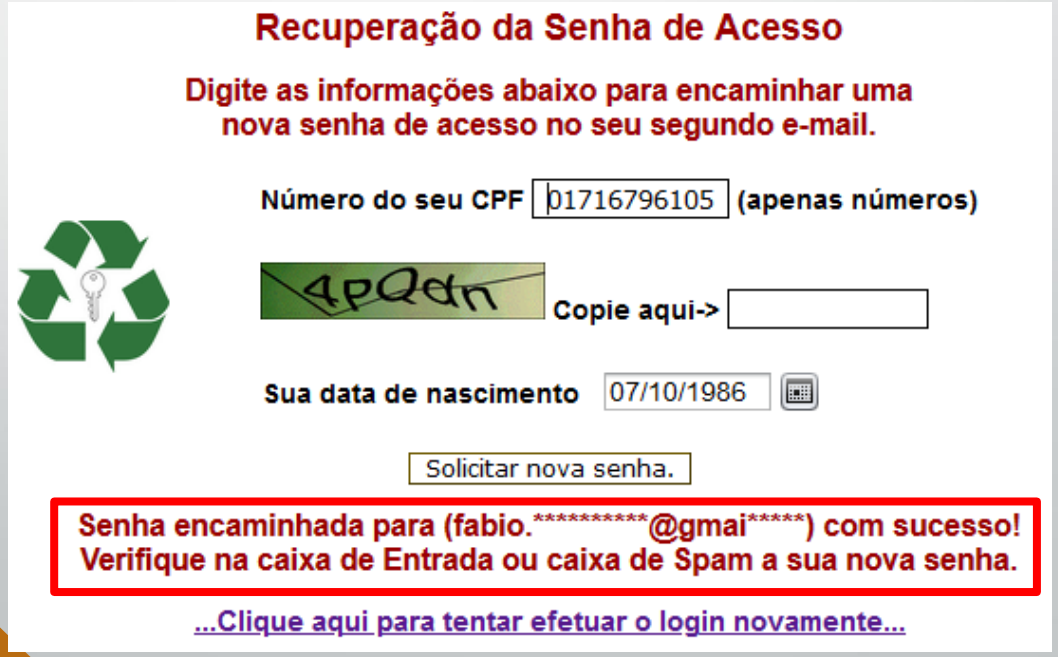


Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha no período solicitado
        - 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".

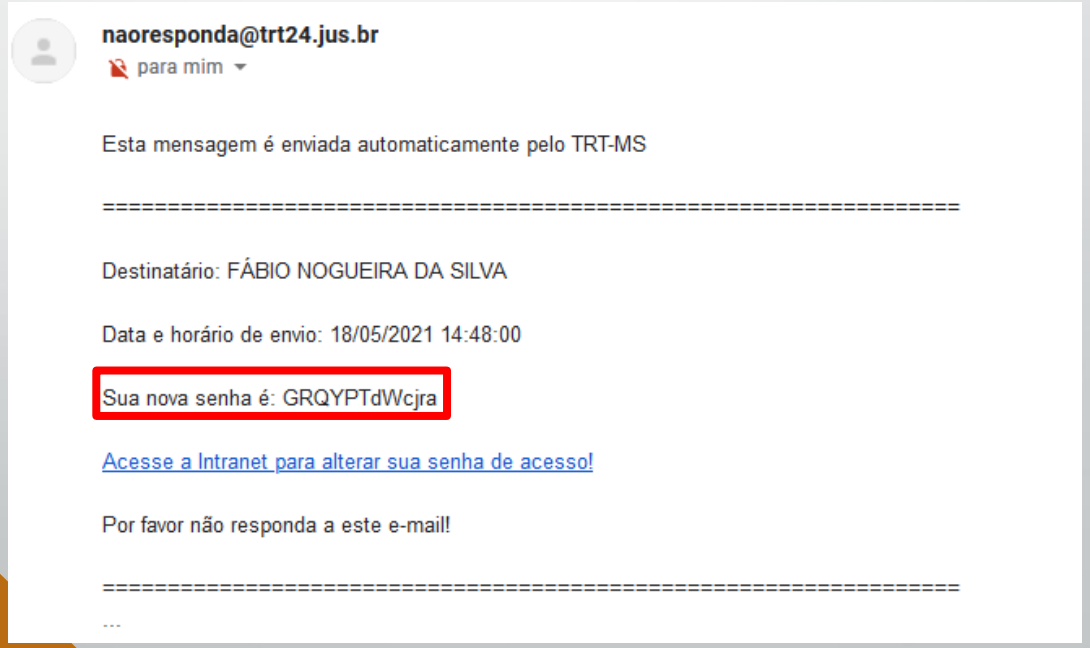
Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha no período solicitado
        - Caso possua e-mail de recuperação cadastrado: Mensagem de "senha encaminhada para (email@pessoal) com sucesso" será mostrada.



Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha no período solicitado
        - 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.



naoresponda@trt24.jus.br
para mim

Esta mensagem é enviada automaticamente pelo TRT-MS

==========

Destinatário: FÁBIO NOGUEIRA DA SILVA

Data e horário de envio: 18/05/2021 14:48:00

Sua nova senha é: GRQYPTdWcjra

Acesse a Intranet para alterar sua senha de acesso!

Por favor não responda a este e-mail!

==========

Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha no período solicitado
        - 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 individuais

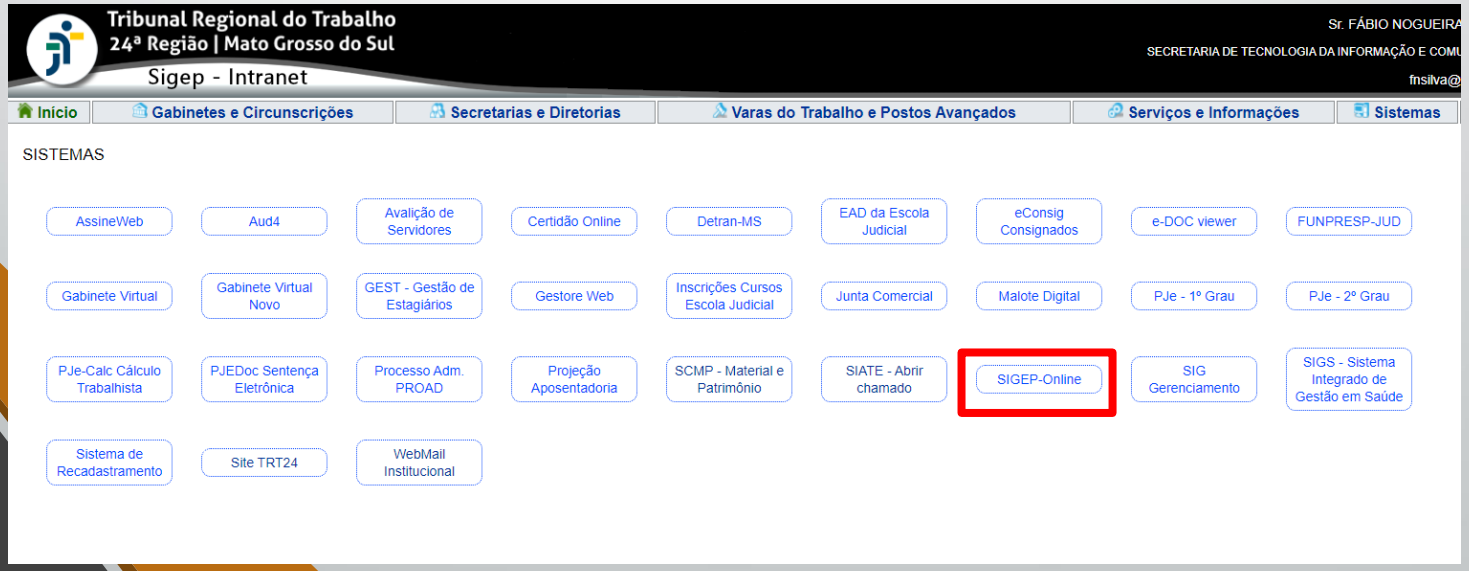
5. Trocar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha no período solicitado
        - Se não possuir e-mail de recuperação cadastrado: **é possível se cadastrar no SIGEP-Online.** Para isso:
            - Entre na nossa intranet em https://intranet.trt24.jus.br

Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha no período solicitado
        - Se não possuir e-mail de recuperação cadastrado: **é possível se cadastrar no SIGEP-Online.** Para isso:
            - Clique na opção "Sistemas" do menu principal

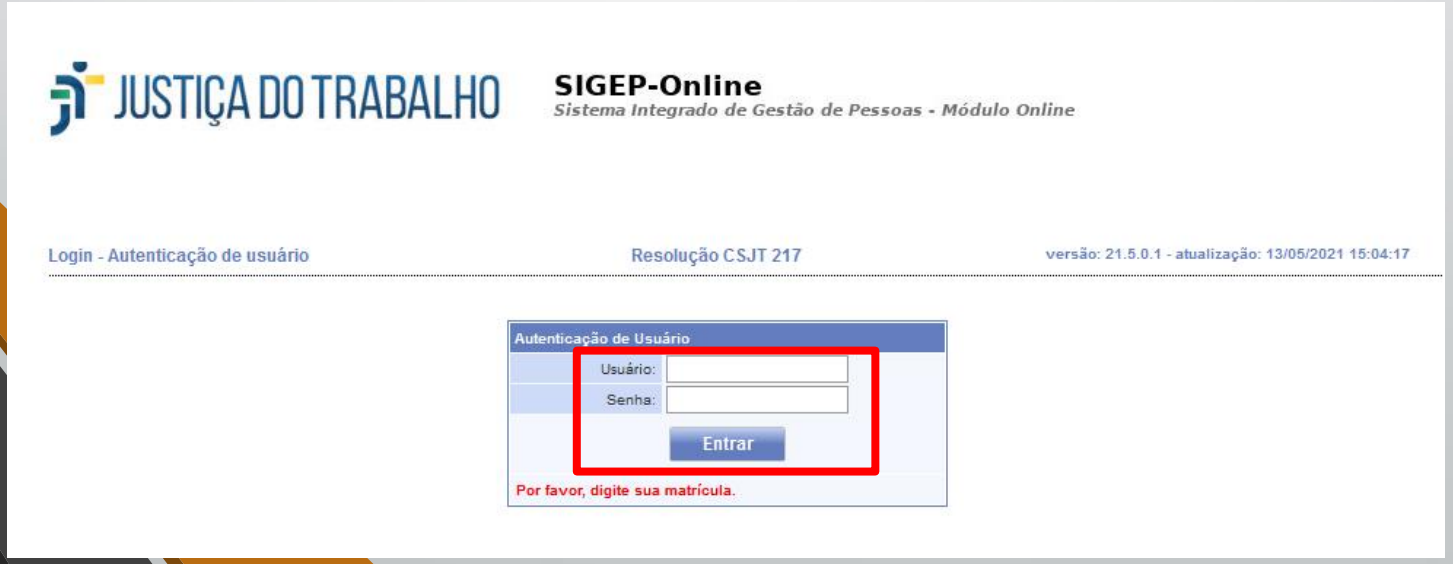
Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – possíveis problemas
   1. Não trocar a senha no período solicitado
      - 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



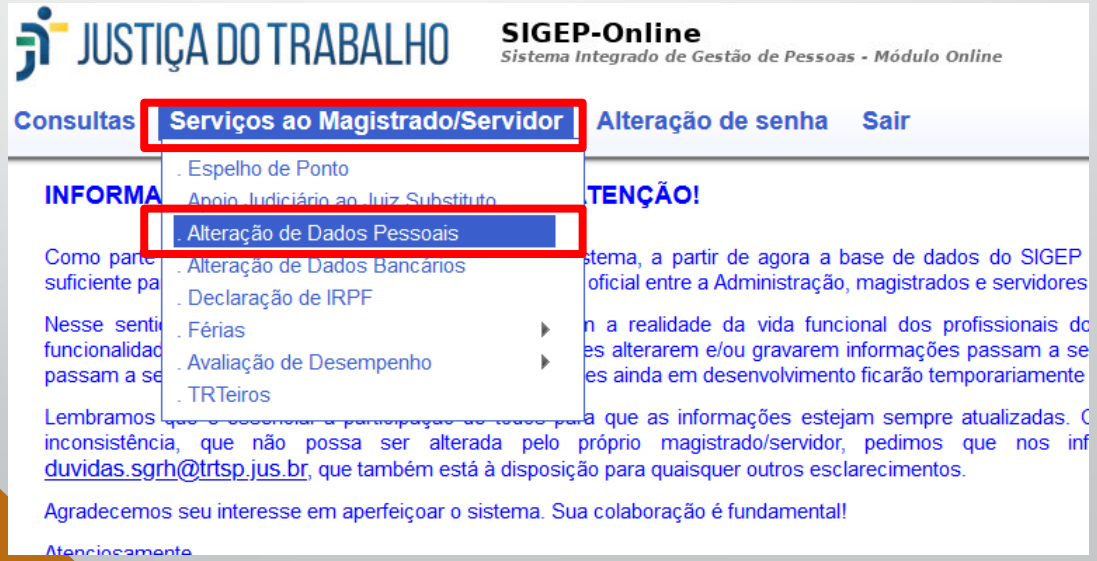
Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha no período solicitado
        - 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.



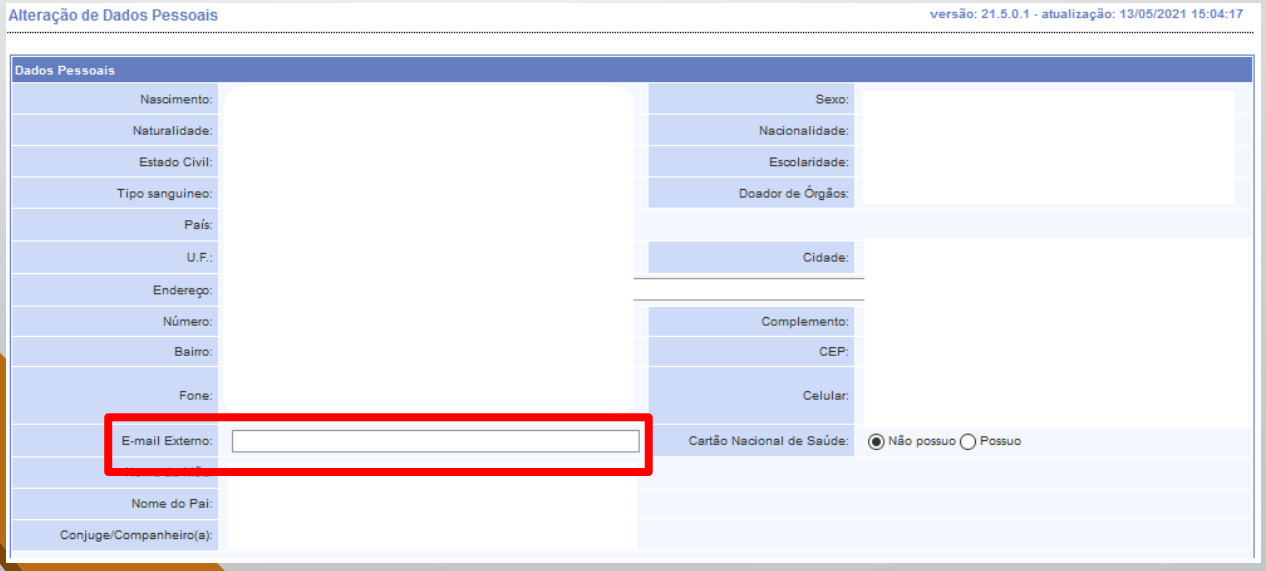
Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha no período solicitado
        - 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 individuais

5. Trocar sua senha na Intranet – possíveis problemas
    1. Não trocar a senha no período solicitado
        - 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 individuais

5. Trocar sua senha na Intranet – possíveis problemas
    2. Máquinas FORA da rede do TRT24
        - 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 individuais

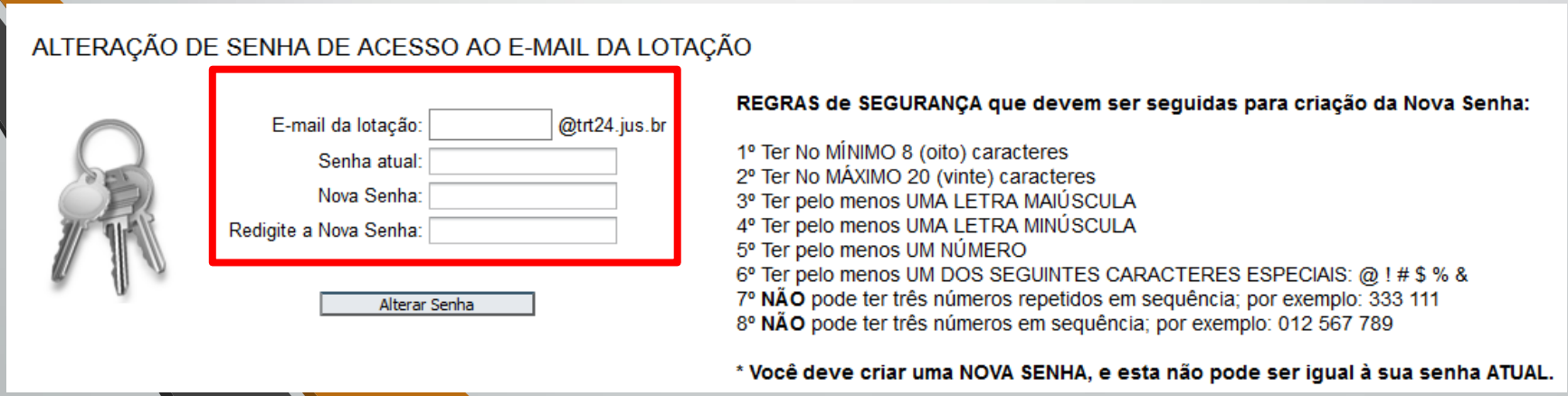
5. Trocar sua senha na Intranet – e-mails setoriais/lotação
   - Os e-mails setoriais também deverão ter as senhas trocadas no período de 24/05 a 28/05.
   - Após o dia 28/05, os e-mails setoriais que não tiverem a senha trocada serão desabilitados.
   - **Para realizar a troca:** acessar https://intranet.trt24.jus.br/

Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – e-mails setoriais/lotação
   - Os e-mails setoriais também deverão ter as senhas trocadas no período de 24/05 a 28/05.
   - **Para realizar a troca:** clicar no ícone "Alterar senha E-mail lotação"

Semana da Segurança da Informação – Ações individuais

5. Trocar sua senha na Intranet – e-mails setoriais/lotação
   - Os e-mails setoriais também deverão ter as senhas trocadas no período de 24/05 a 28/05.
   - **Para realizar a troca:** preencher os campos "E-mail lotação", "Senha atual", "Nova Senha", "Redigite a Nova Senha". Clicar no botão "Alterar Senha"



Semana da Segurança da Informação – Ações individuais

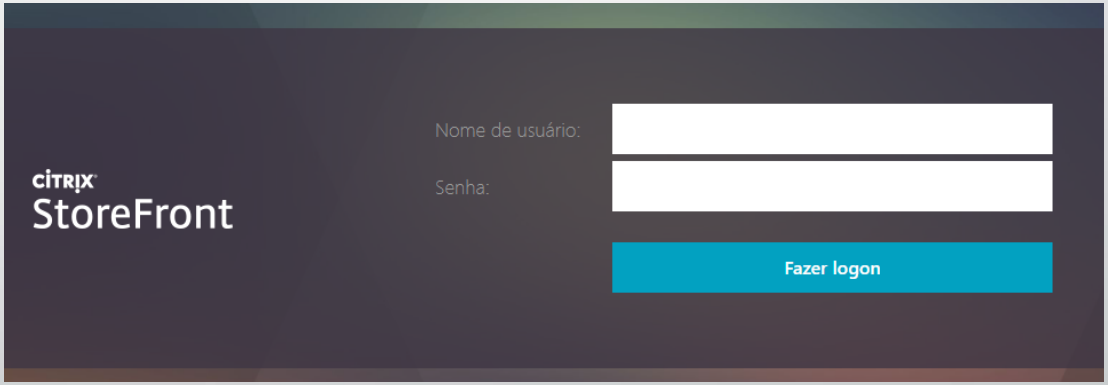
6. Não utilizar mais usuários genéricos e compartilháveis
   - Impossível de estabelecer relação com um único usuário, já que todos usam.
   - A senha compartilhada gera muito mais oportunidades de vazamento.
   - Impossível auditar as atividades desses usuários genéricos
   - Serão desabilitados durante a semana da segurança da informação.

Semana da Segurança da Informação – Ações individuais

7. Acesso remoto a sua estação deverá ser autorizado e acompanhado em tempo integral por você.
   - Não será mais possível o acesso dos técnicos da SETIC ao seu computador sem consentimento expresso.
   - É sua responsabilidade acompanhar o acesso de suporte em todas as suas etapas.
   - Exija o número do chamado (SIATE) como maneira de confirmar a identidade dos técnicos da TI

Semana da Segurança da Informação – Ações individuais

8. O gabinete virtual antigo será DESATIVADO.
   - Não será mais possível acessar o gabinete virtual antigo para o teletrabalho - https://gabinetevirtual.trt24.jus.br/
   - Somente o novo gabinete virtual, com a versão mais atualizada, estará acessível em https://gabvirtual.trt24.jus.br/
     - Caso tenha problemas para configurar o novo gabinete, será necessário a abertura de um SIATE.



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/