

CYBER SECURITY

VOCÊ SABE COMO PROTEGER OS DADOS DA SUA EMPRESA?

PAINELISTAS

RAFAELLO ROSS E VINÍCIUS FERREIRA - POLÍCIA CIVIL

PEDRO HENRIQUE ARAÚJO - TIGRE

DIEGO CONTEZINI - ASAAS

CHARLES CHRISTIAN MIERS - UDESC

ALEX MASSIA CANAL - NIDEC

19 DE AGOSTO 18H30 SEDE ACIJ

ESPAÇO EMPRESARIAL E COQUETEL



Fischer
Advocacia
www.fischeradvocacia.com



REALIZAÇÃO



Economia Forte, Cidade Feliz



Economia Forte, Cidade Feliz

O quê é segurança?

A segurança da informação e a segurança de dados **parece** ser um tema de domínio público...



O quê é segurança?

Diferentes entendimentos do quê é segurança:

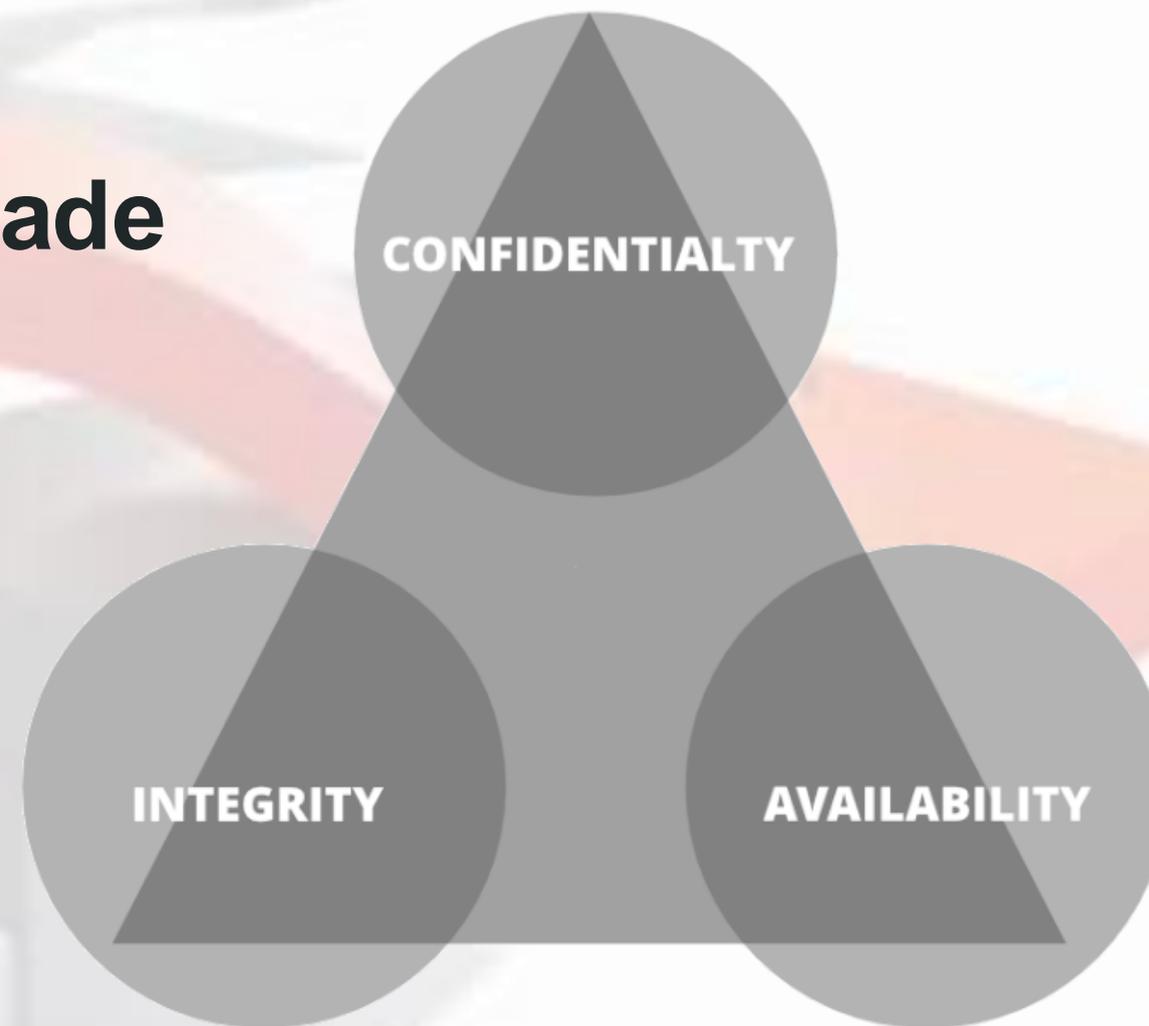
- Interpretação de um diretor
- Interpretação de um gerente
- Interpretação de profissionais do departamento de TI
- Interpretação de um colaborador
- Interpretação de um comerciante
- Interpretação de um cidadão



O quê é segurança?

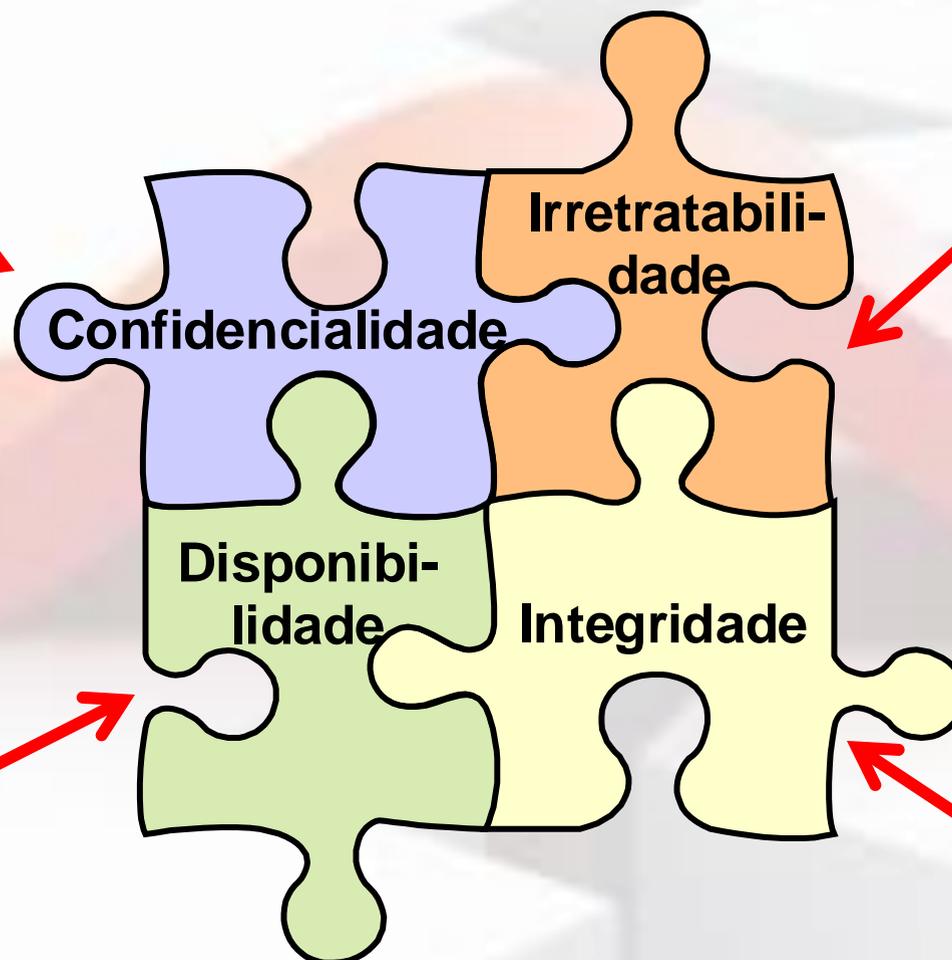
Tríade CIA:

- **Confidentiality / Confidencialidade**
- **Integrity / Integridade**
- **Availability / Disponibilidade**

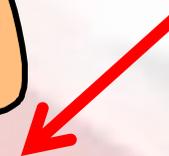


O quê é segurança?

Dados só devem ser acessados por quem for comprovadamente permitido



Comprovar que realmente é quem diz ser, comprovando a identidade



Os dados devem estar sempre disponíveis para serem acessados pelos usuários legítimos



Manter os dados fiéis ao autor real / estado original



O quê é segurança?

Objetivos da segurança:

- Reduzir riscos
- Manter os riscos dentro dos limites aceitáveis
- Economizar dinheiro, através de ações pró-ativas
- Estabelecer planos para quando incidentes ocorrerem
- Assegurar-se / comprovar a real situação de segurança



O quê é risco?



Possibilidade de um ativo sujeitar-se a fatores e incidentes que possam resultar em perdas ou danos, comprometendo a continuidade das atividades de uma organização

O quê é risco?

Ativo: algo tem que valor para uma organização



Possibilidade de um ativo sujeitar-se a fatores e incidentes que possam resultar em perdas ou danos, comprometendo a continuidade das atividades de uma organização

**Perdas ou Danos:
Consequências**

Fatores e Incidentes:

- **Vulnerabilidades: fraquezas na segurança**
- **Ameaças: possibilidade de exploração de vulnerabilidades**

O quê é risco?

Risco

=

Vulnerabilidades

X

Ameaças



Nível de Risco

=

Risco

X

Valor dos ativos

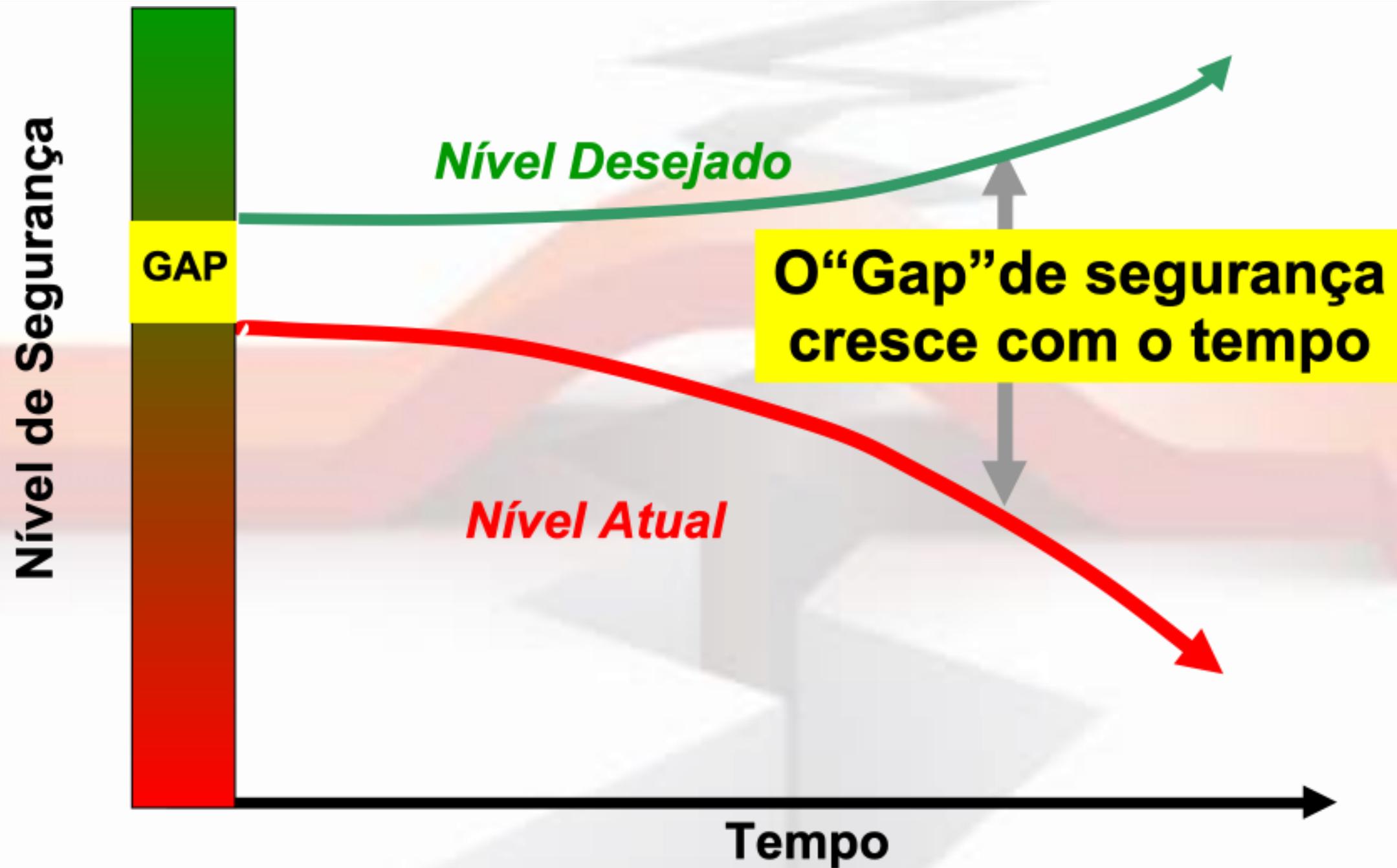
X

Consequências



Se você não puder medir o risco, você não poderá reduzi-lo!

O quê é risco?



Normas/Leis/Recomendações

Diversas e com escopos:

- **LGPD – Lei Geral de Proteção de Dados**
- **Marco Civil Internet**
- **GDPR - General Data Protection Regulation**
- **HIPAA - Health Insurance Portability and Accountability Act**
- **NIST – Cybersecurity Framework**
- **Família ISO 27000, COBIT, ...**



Como mitigar os riscos?

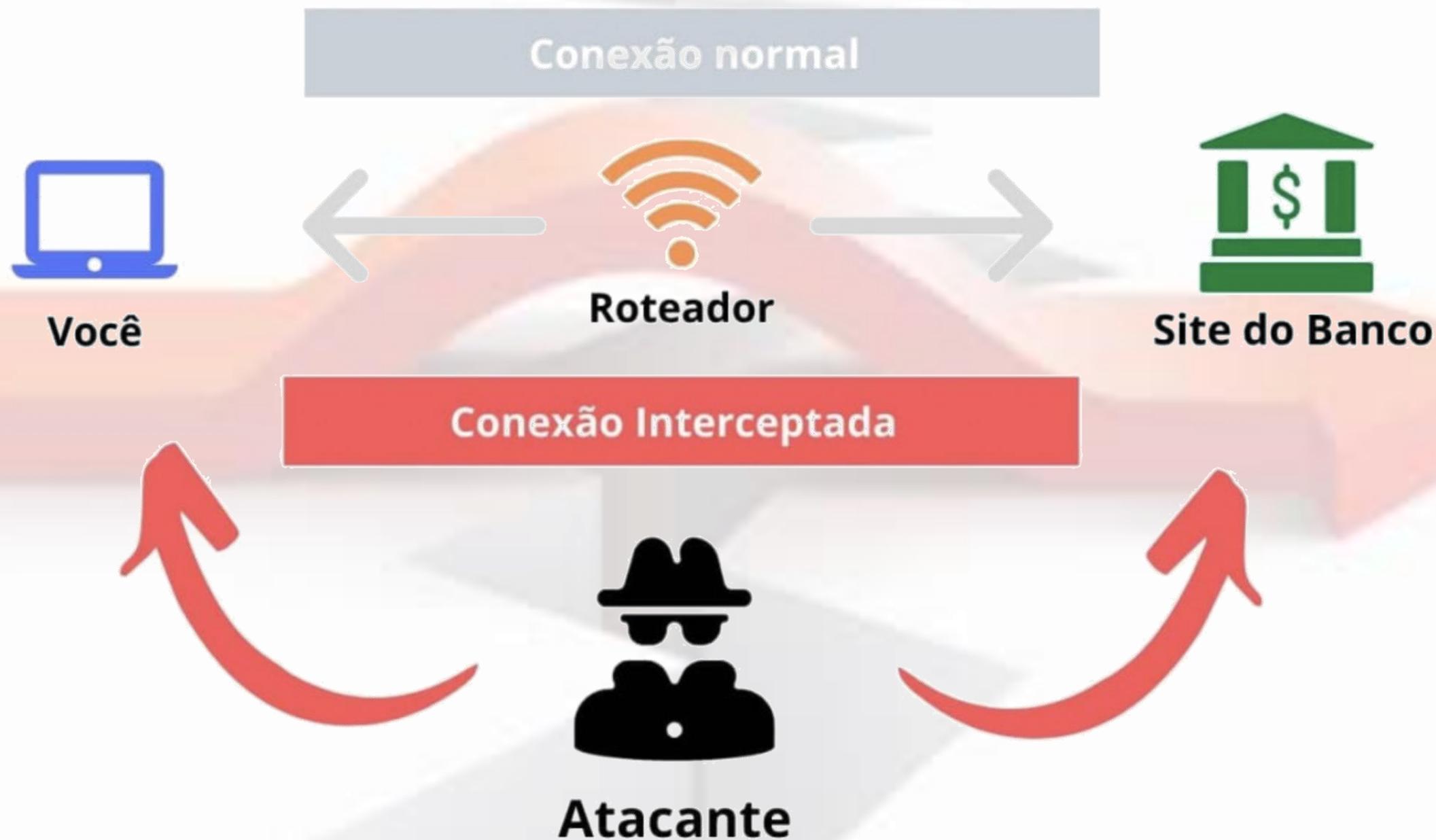
Segurança é um processo, não uma ação ou item isolado:

- Melhor software do mundo configurado indevidamente gera risco
- Pessoas são a parte mais importante e vulnerável desse processo
- **Prevenir, prevenir e prevenir... Prevenir é mais barato e eficiente do que reagir...**
- **Incidentes de segurança IRÃO ocorrer, plano de ação é necessário! Estar preparado e treinado para cumprir planos!**



(In)Segurança nas empresas?

Redes sem fio (IEEE 802.11 aka WiFi) :



(In)Segurança nas empresas?

Celulares:

- Quais informações estão no seu celular?
- O quê você deixa de fazer sem o seu celular?
- O quê um atacante pode fazer com o seu celular?
- Qual seu plano de recuperação na perda ou comprometimento do seu celular?
- Ataques MitM em aeroportos, shoppings, locais públicos, e sua casa!



Como obter mais informações?

Locais de informação:

- Buscar canais oficiais, certificar-se se é realmente quem diz ser...
- Atacantes pagam patrocínio em mecanismos de busca e redes sociais (e.g., Google, Instagram)

A screenshot of a Google search for "detran sc". The search results show a sponsored link for "transiltosc.inicioscscritoriobemvindo.com" and a link for "DetranSC" with the text "Despachante 2024/SC — Qualidade no Atendimento, Anos de Experiência, Seriedade no que Faz. Consulta...". Below this, there are links for "Veicular 2024" (Santa Catarina Emitir Guia) and "SC 2024" (Inicio Bem Vindo). At the bottom, there is a link for "DETTRAN – SC" with the URL "https://www.detran.sc.gov.br".

A screenshot of the DETRAN/SC website showing a "Consulta Consolidada do Veículo". The page displays fields for "Renavam:" and "Placa:". A modal window titled "Pagamento com Pix" is overlaid on the page, showing a QR code and a table of payments. The table lists the following items and amounts:

Discriminação	Valor em Reais (R\$)
Licenciamento Anual 2024	R\$ 149,37
IPVA (2a. Cota) 2024	R\$ 280,64
IPVA (3a. Cota) 2024	R\$ 280,64

The modal also shows the date "Data: 03/07/2024" and the total value "Valor: R\$ 280,64". A QR code is displayed with the Pix code "00020126580014BR.GOV.BCB.PIX01366daa9ad5-00be-419d-a673-".



Como obter mais informações?

Locais de informação:

- <https://internetsegura.br/>



Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!

para Crianças para Adolescentes para Pais e Educadores para 60+ para Técnicos para Interesse Geral

perfil @InternetSeguraBR

Se proteger de vazamentos de dados, falhas de sistemas e *links* maliciosos não tem sido fácil para você?

Segue o @InternetSeguraBR no Instagram! Lá você encontra muitas dicas e informações essenciais sobre como usar a Internet com segurança.

Compartilhe com amigos, colegas ou familiares e junte-se a nós na missão de promover uma #InternetSegura para todos!

Como obter mais informações?



Delitos praticados por meios eletrônicos

Perguntas e respostas



Boleto falso



2. Boleto Falso

O golpe ocorre da seguinte forma:

O boleto de cobrança é um instrumento de pagamento pelo qual o emissor, denominado "Beneficiário", receberá em sua conta o valor referente a um produto ou serviço.

O criminoso, valendo-se de engenharia social ou de um link fraudulento, altera o código de barras de modo que o valor caia na conta do integrante da quadrilha.

Como evitar o golpe:

- Verifique se os dados do "Beneficiário" correspondem aos de quem lhe vendeu o produto ou serviço.
- Confira se os três primeiros números do código de barras correspondem ao banco cuja logomarca aparece no boleto.
- Desconfie se o código de barras estiver com falhas que apresentem espaços excessivos entre as barras ou qualquer outra alteração que impossibilite o reconhecimento pela leitora.
- Sempre que tiver dúvidas sobre a veracidade de um boleto de cobrança, consulte diretamente o fornecedor que o emitiu.
- Evite reimprimir boletos de cobrança em sites que não sejam do banco emissor do boleto. Evite negociar valores de descontos de boletos com pessoas estranhas, ou que se identifiquem como funcionários dos bancos ou de empresas de cobrança.

Caso tenha sido vítima, o que fazer:

- Entre em contato com o banco e tente bloquear o valor.
- Tire cópia do comprovante de pagamento e demais documentos correlatos.
- Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica <https://www.delegaciaeletronica.policiaacivil.sp.gov.br/esp-de-cidadado/home> na opção OUTROS CRIMES.

Clonagem de Whatsapp



1. Clonagem de WhatsApp

O golpe ocorre da seguinte forma:

O criminoso liga ou envia uma mensagem se passando por um funcionário de site de compra ou de um banco e diz que estará encaminhando um código promocional ou código de confirmação. Ele pede para que a vítima informe esse código que, na verdade, é a verificação do WhatsApp e com ele o criminoso consegue clonar a conta do consumidor.

Após a clonagem, o criminoso passa a enviar mensagens para os contatos da vítima, se passando por ela, pedindo dinheiro. As desculpas para solicitar dinheiro emprestado são as mais diversas, e na maioria das vezes os alvos principais da investida são os parentes mais próximos e amigos que, acreditando na mensagem, acabam depositando ou transferindo valores seguindo as coordenadas do criminoso.

Como evitar o golpe:

- Ative a "Confirmação em duas etapas" no WhatsApp. Acesse o link e veja como: https://faq.whatsapp.com/about-real-verification/about-two-step-verification?lang=pt_br
- NUNCA forneça o código verificador que você recebe via SMS em seu celular.
- Não instale apps de terceiros ou compartilhe informações pessoais a pedido de ninguém pelo whatsapp.
- Desconfie de situações em que a pessoa solicita a realização de transferências e pagamentos em caráter de urgência.
- Ligue para a pessoa que solicitou o dinheiro e verifique se realmente é ela quem está solicitando a transação.

Caso tenha sido vítima, o que fazer:

- Vítima do celular clonado
- Envie um e-mail para support@whatsapp.com com o assunto "CONTA HACKEADA - DESATIVAÇÃO DE CONTA". Relate o ocorrido e siga as instruções do provedor.
 - Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica <https://www.delegaciaeletronica.policiaacivil.sp.gov.br/esp-de-cidadado/home> na opção OUTROS CRIMES.
 - Peça para amigos e familiares excluírem o telefone clonado de grupos e alertarem o máximo de contatos em comum sobre o ocorrido.

Vítima foi quem fez o pagamento

- Entre em contato com o banco e tente bloquear o valor.



Fraudes bancárias

3. Fraudes bancárias

Alguns tipos de fraudes bancárias mais recorrentes:

Falso funcionário ou falsa central de atendimento: O estelionatário finge ser funcionário da instituição financeira e diz estar com problemas no cadastro ou irregularidades na conta. A vítima fornece informações sobre sua conta, e com isso o bandido realiza transações fraudulentas.

Falso motoboy: Integrantes da quadrilha ligam para a vítima e dizem pertencem a central de relacionamento do banco. Afirmando que houve problemas com o cartão da vítima e pedem que ela digite sua senha numérica no teclado do telefone. Na sequência, dizem que enviaram um motoboy na casa da vítima para pegar o cartão. Em posse do cartão e a senha, realizam operações espúrias.

Phishing: O criminoso envia links, e-mails e SMS para a vítima com mensagens que, na maioria das vezes, exploram as emoções (curiosidade, oportunidade única, medo, etc), fazendo com que ela clique nos links e anexos que subtraem dados pessoais ou induzem a realizar cadastros ou fornecer informações.

Como evitar o golpe:

- Evite usar computadores públicos e redes abertas de wi-fi para acessar conta bancária ou fazer compras online.
- NUNCA abra e-mails de origem ou de procedência duvidosa.
- Não execute programas, abra arquivos ou clique em links que estejam anexados ou no corpo desses e-mails.
- Deleite esses e-mails e, caso tenha clicado em alguma parte deste e-mail e executado um programa, comunique imediatamente ao seu banco o ocorrido e altere todas as suas senhas de acesso à sua conta bancária em outro computador confiável, ou no mesmo, após uma verificação completa de infecção de vírus por um técnico confiável.
- NUNCA utilize seu cartão para fazer compras em sites desconhecidos.

Caso tenha sido vítima, o que fazer:

- Entre em contato com o banco e tente bloquear o valor.
- Tire cópia do comprovante de pagamento e demais documentos correlatos.



CYBER SECURITY

VOCÊ SABE COMO PROTEGER OS DADOS DA SUA EMPRESA?

PAINELISTAS

RAFAELLO ROSS E VINÍCIUS FERREIRA - POLÍCIA CIVIL

PEDRO HENRIQUE ARAÚJO - TIGRE

DIEGO CONTEZINI - ASAAS

CHARLES CHRISTIAN MIERS - UDESC

ALEX MASSIA CANAL - NIDEC

19 DE AGOSTO 18H30 SEDE ACIJ

ESPAÇO EMPRESARIAL E COQUETEL



Fischer
Advocacia
www.fischeradvocacia.com



REALIZAÇÃO



Economia Forte, Cidade Feliz



Economia Forte, Cidade Feliz