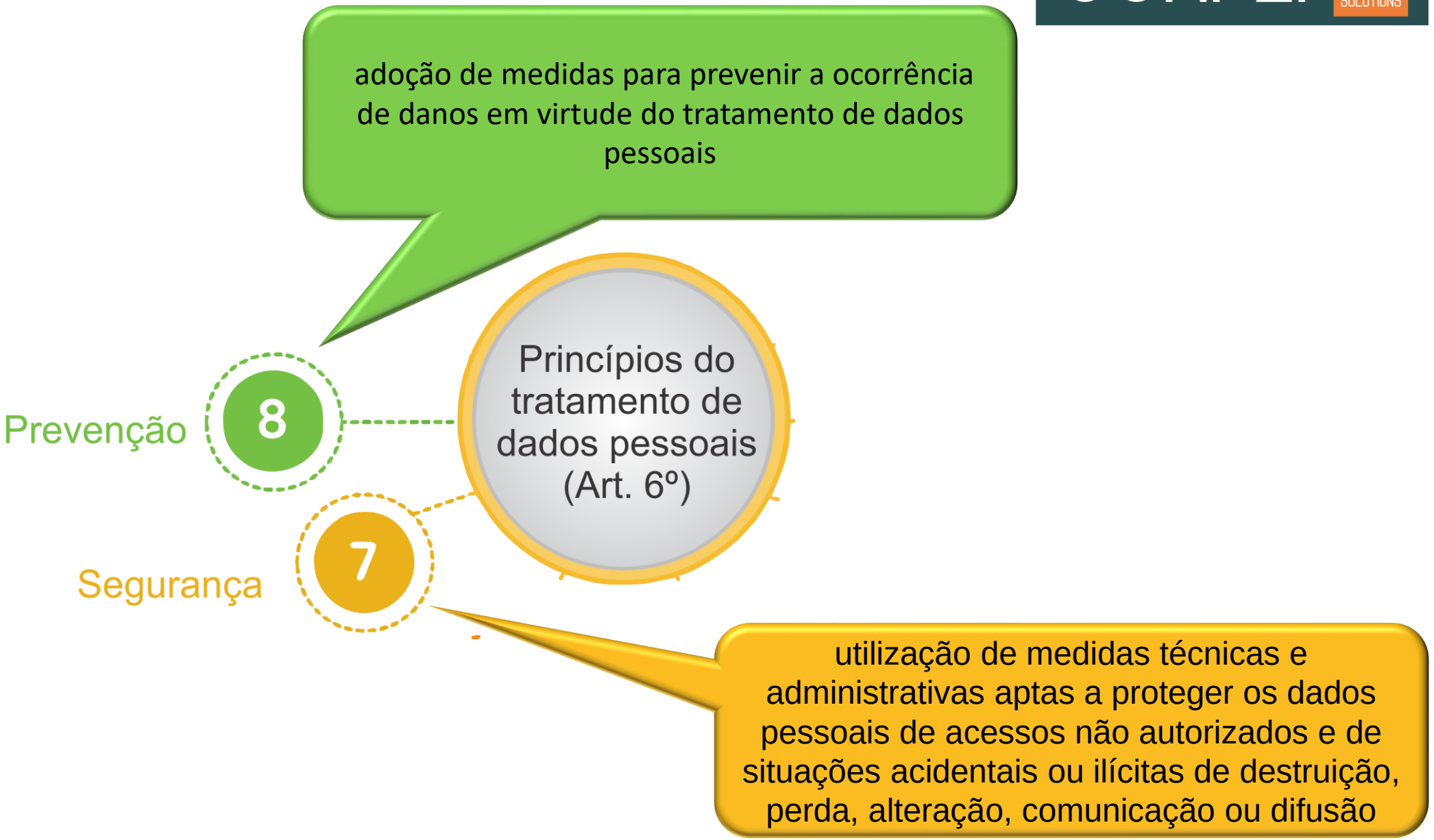
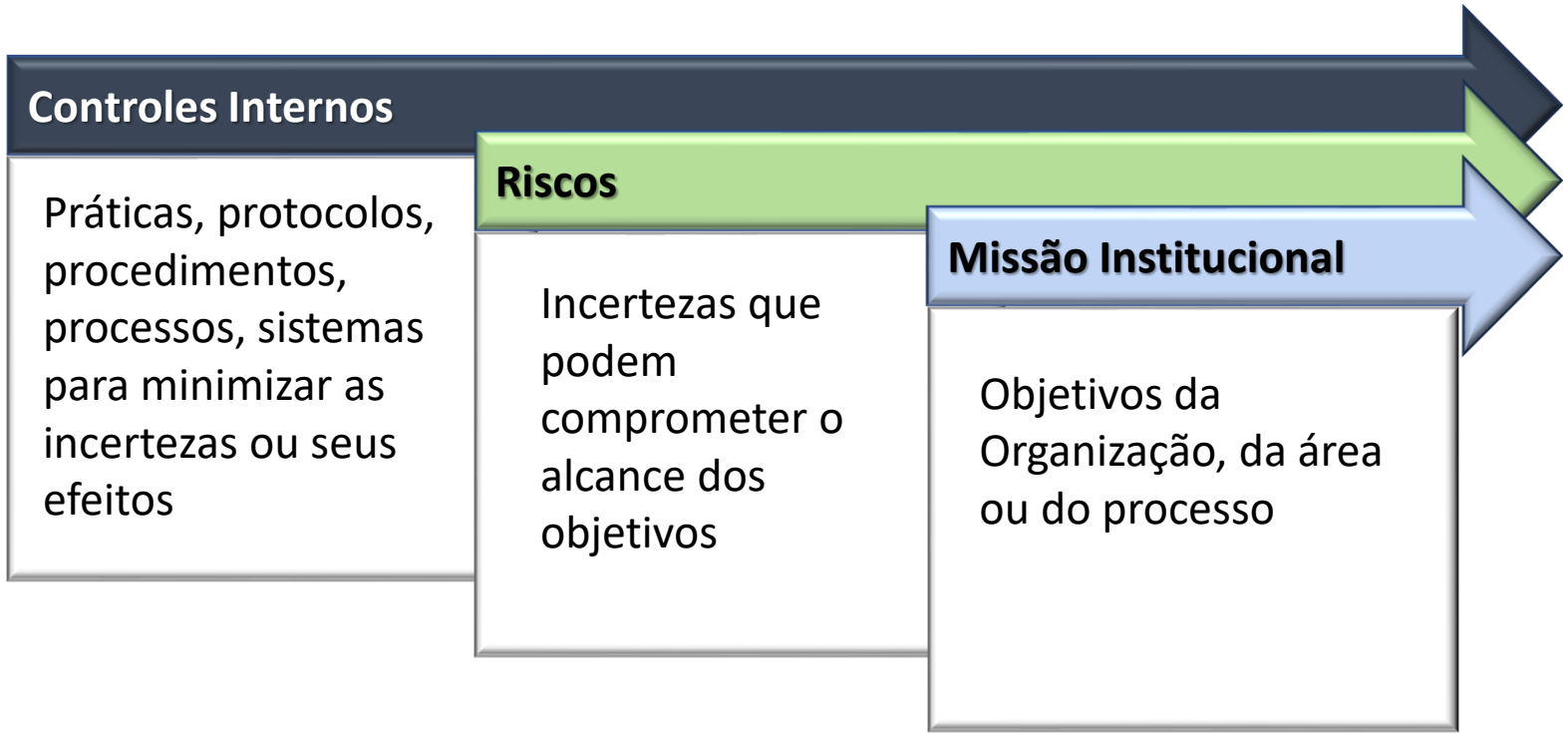

Princípios do tratamento de dados pessoais (Art. 6º)
1
Finalidade
2
Adequação
3
Necessidade
4
Livre acesso
5
Qualidade dos dados
6
Transparência
7
Segurança
8
Prevenção
9
Não discriminação
10
Responsabilização e prestação de contas


adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais
Princípios do tratamento de dados pessoais (Art. 6º)
Prevenção
8
Segurança
7
utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão


Controles Internos
Práticas, protocolos, procedimentos, processos, sistemas para minimizar as incertezas ou seus efeitos
Riscos
Incertezas que podem comprometer o alcance dos objetivos
Missão Institucional
Objetivos da Organização, da área ou do processo

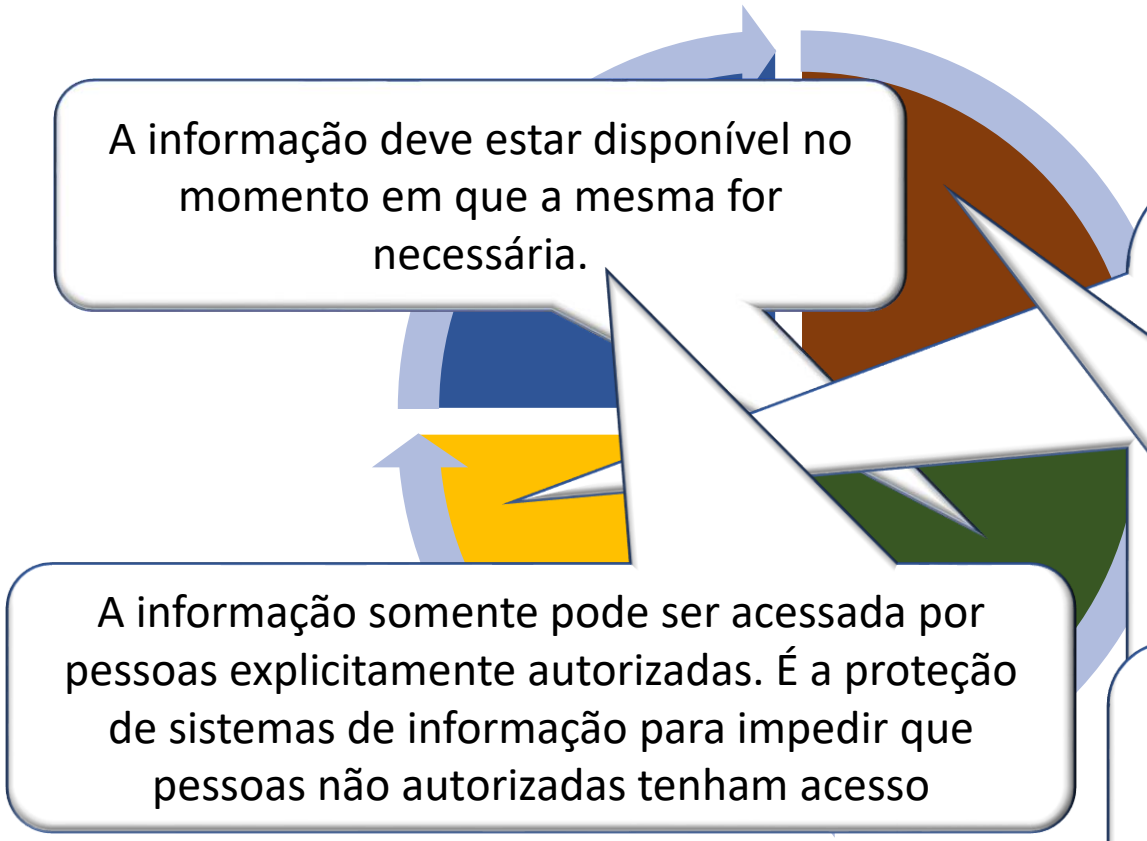
Probabilidade

Impacto

AVALIAÇÃO DE RISCOS

TRATAMENTO DOS RISCOS

PERSPECTIVAS DE RISCOS



A informação deve estar disponível no momento em que a mesma for necessária.

A informação somente pode ser acessada por pessoas explicitamente autorizadas. É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso

A informação coletada deve ser necessária (limitação ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não essivos em relação às finalidades), ter **propósitos legítimos** specíficos, explícitos e informados ao titular, sem de de tratamento posterior de forma incompatível lidades) e ter assegurada a sua **anonimização** íveis no do perde a ndivíduo).

A informação deve ser recuperada em sua forma original (no momento em que foi armazenada). É a proteção dos dados ou informações contra modificações intencionais ou acidentais não autorizadas

Lei 13.709:2018

ISO 27001 : 2013 - 6.1.2.c.1

ISO 27701 : 2019 - 5.4.1.2

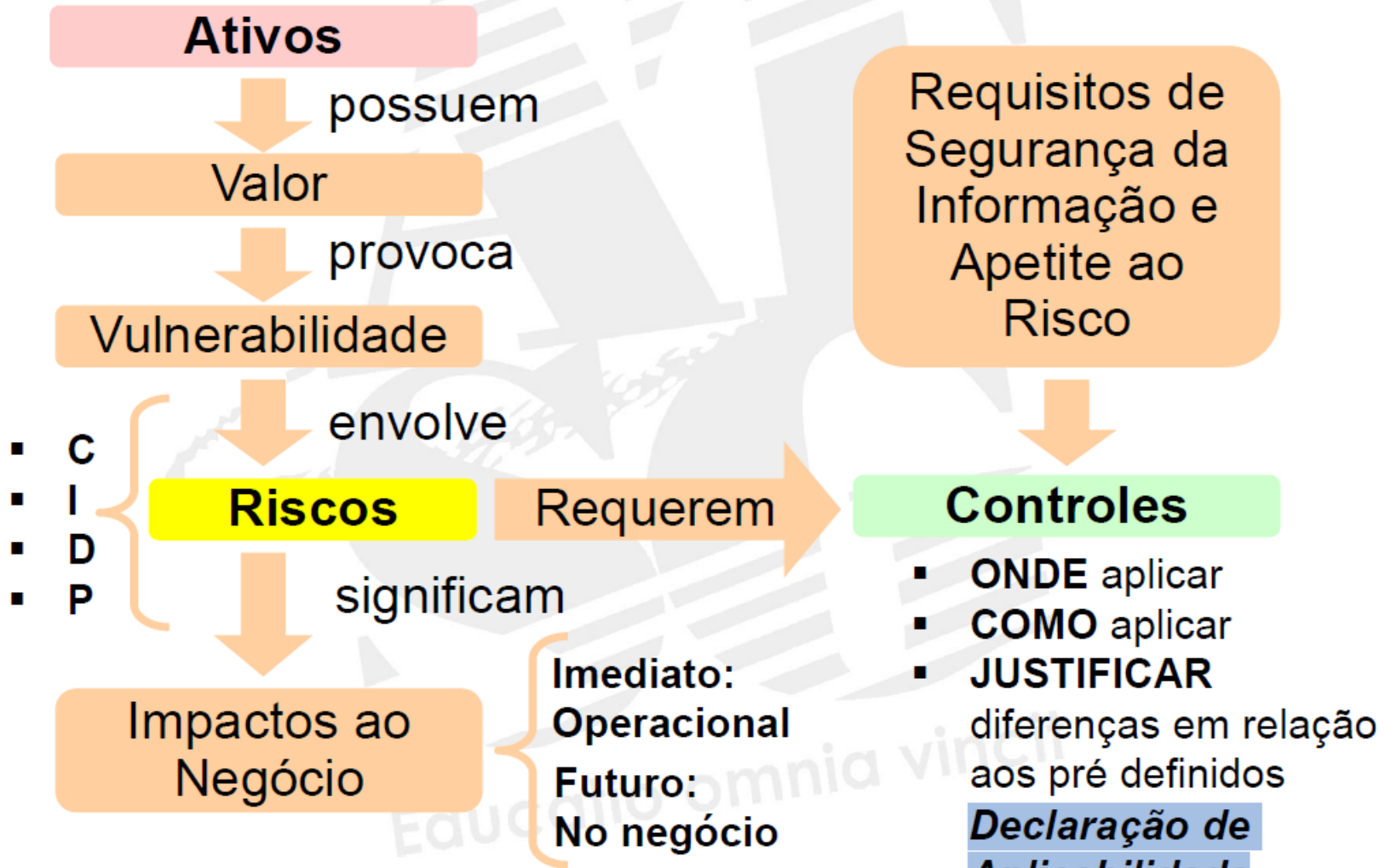
PERSPECTIVAS DE RISCOS

- Confidencialidade
- Integridade
- Disponibilidade
- Privacidade

ISO 27001 : 2013 – 6.1.2.c.1

ISO 27701 : 2019 – 5.4.1.2

Compreendendo a "lógica" da ISO 27001



EXEMPLOS DE RISCOS

- Acesso não autorizado
- Falha ou erro de processamento
- Uso indevido
- Modificação não autorizada
- Perda
- Reidentificação de dados pseudonimizados
- Remoção não autorizada
- Roubo
- Sequestro de dados

TIPOS DE CONTROLES

Administrativos

- Desenvolvimento de estudos
- Política de segurança da informação
- Conscientização e treinamento de recursos humanos em TIC
- Gerenciamento de contratos

Técnicos

- Controle de acesso
- Segurança dos dados pessoais armazenados
- Segurança das comunicações
- Manutenção de programa de gerenciamento de vulnerabilidades
- Medidas relacionadas ao uso de dispositivos móveis
- Medidas relacionadas ao serviço em nuvem
- Versões atualizadas dos sistemas e adequadamente configuradas
- Senha forte - dupla autenticação quando possível
- Não instalar produtos sem saber o que está instalando
- Usar criptografia sempre que possível

BOAS PRÁTICAS PARA O DESENVOLVIMENTO DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS:

Identificar e mensurar as vulnerabilidades

Criar Métricas para verificar a resiliência do negócio, exemplo: “quanto tempo o site pode ficar fora do ar?“

Armazenamento da Informação para avaliar qual informação deverá ser mantida

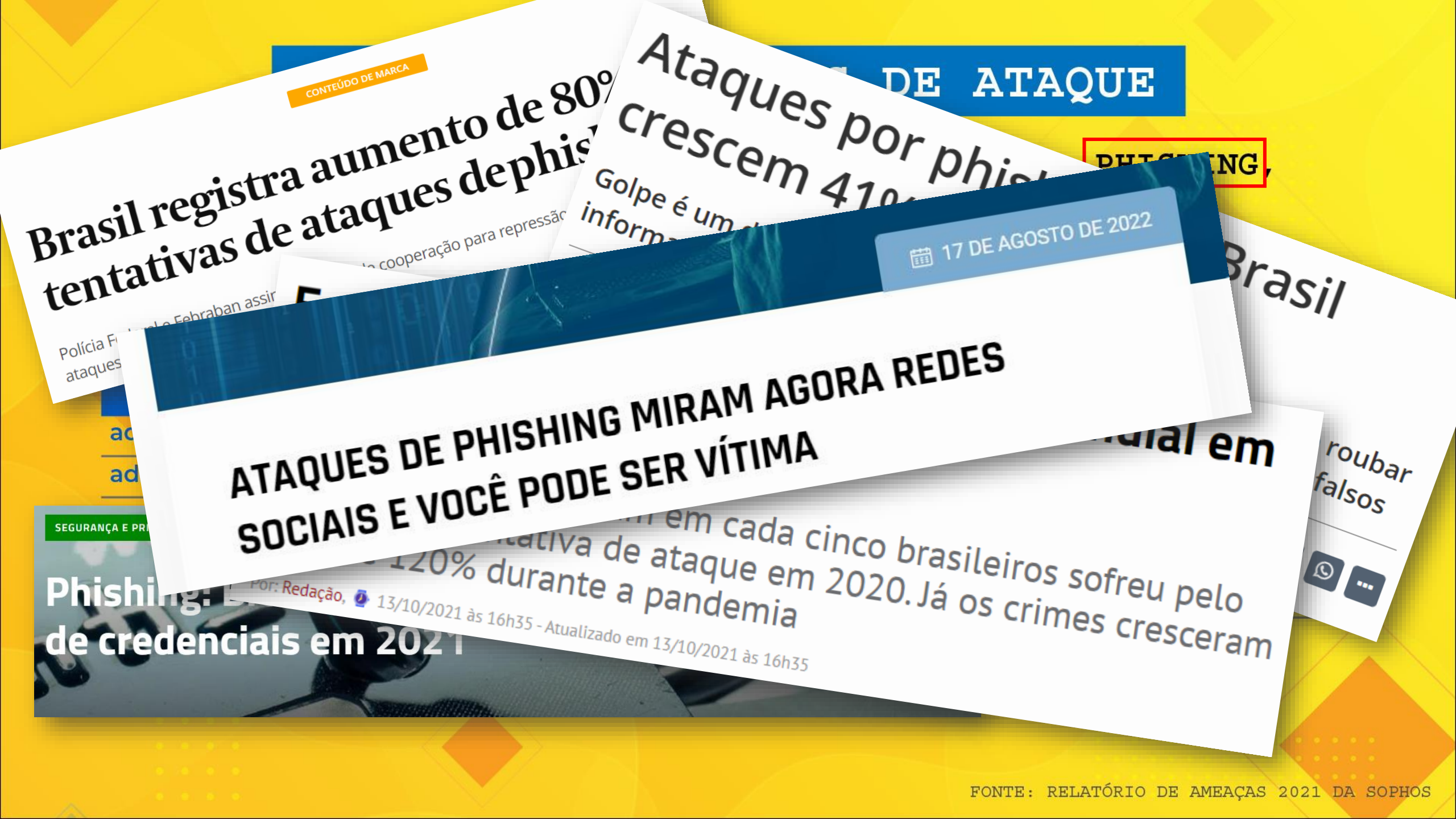
Escolha da Segurança deve-se pautar na confiança, daquele parceiro que vai ser o melhor nos momentos de crise.

Maturidade, os responsáveis pela empresa devem trabalhar para conscientizar até o menor nível, e para isso deve haver,

Comunicação entre todos os funcionários, para que qualquer problema possa ser relatado e tratado.

BOAS PRÁTICAS PARA O INDIVÍDUO NA SEGURANÇA DA INFORMAÇÃO:

- Escolha senhas fortes;
- Nunca divulgue ou compartilhe senhas pessoais;
- Alteração periódicas de suas senhas;
- Preferencialmente não utilizar senhas iguais para serviços diferentes;
- Bloquear a estação de trabalho ao se ausentar;
- Utilize a autenticação de dois fatores;
- Leia as políticas de privacidade e uso do aplicativo;
- Mantenha antivírus sempre atualizado e pleno funcionamento;
- Não ignore notificações sobre detecção de ameaça;
- Mantenha opção de backup ativada;
- Cuidado com redes de wi-fi não seguras;
- Não abrir e-mail de remetentes desconhecidos;
- Sempre verifique a URL dos sites que irá acessar.
- Não insira seus dados pessoais em sites duvidosos;
- Mantenha-se atualizado sobre boas práticas de segurança da informação.



FONTE: RELATÓRIO DE AMEAÇAS 2021 DA SOPHOS

Phishing

O QUE É?

O phishing é um crime cibernético em que os bandidos assumem falsamente a identidade de um remetente legítimo, induzindo as vítimas a fornecer informações confidenciais, como senha e detalhes bancários. Os ataques de phishing são comumente iniciados por meio de falsificação de e-mail.

1 a cada 10 mensagens são bem-sucedidas

Ataques direcionados podem afetar as finanças de uma empresa, bem como sua reputação. Eles podem resultar em violações de dados, o que por sua vez pode custar até milhões e dólares.

COMPLY LGPD SOLUTIONS

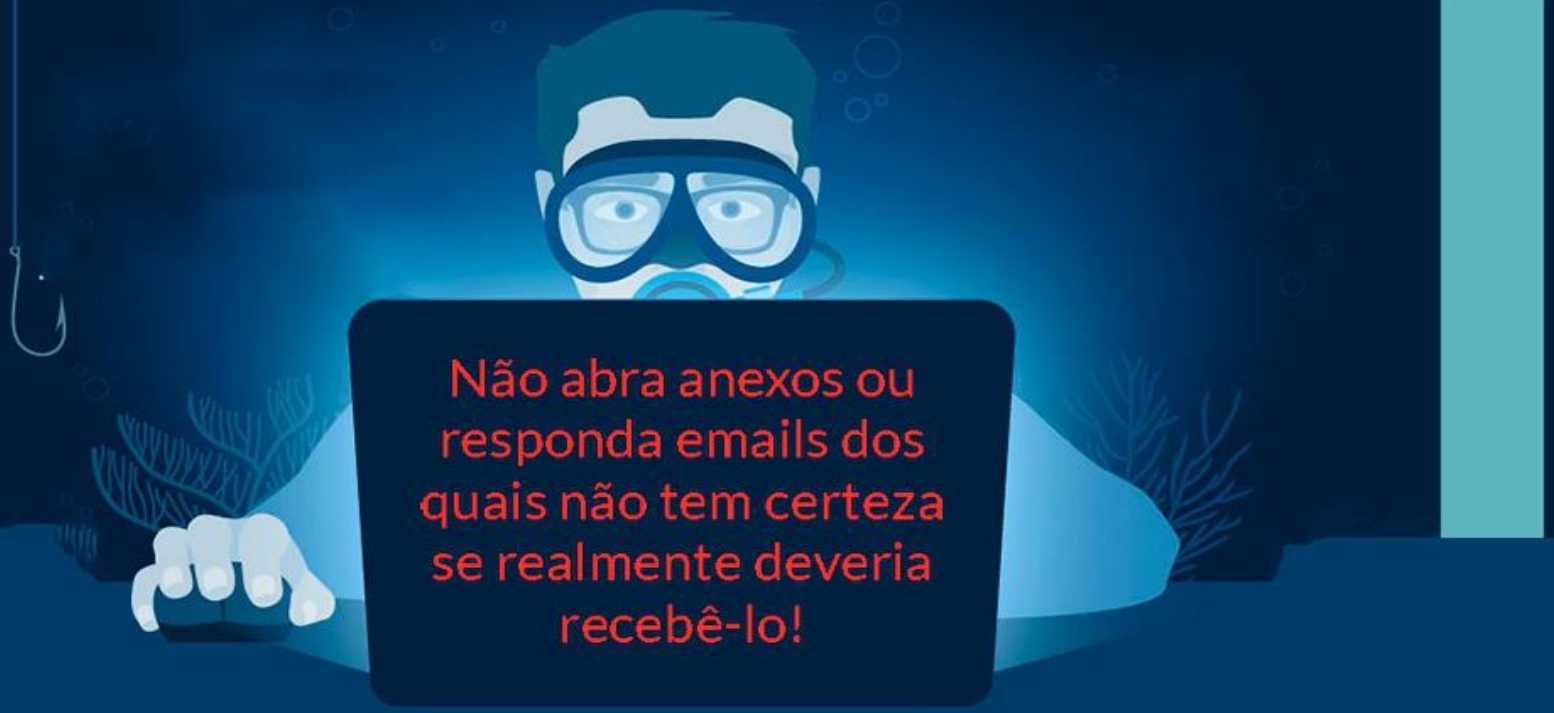
1 Atacantes reúnem informações sobre indivíduos na empresa-alvo.

2 Usando as informações coletadas, uma mensagem de e-mail é criada especificamente para o alvo. O e-mail pode vir com um anexo ou link malicioso.

2 Usando as informações coletadas, uma mensagem de e-mail é criada especificamente para o alvo. O e-mail pode vir com um anexo ou link malicioso.

Os criminosos mascaram campos, fazem o e-mail de origem parecer verdadeiro,
mas na realidade é tudo uma enganação, falsificação.
O e-mail de origem é outro, está mascarado
e não aparece ao usuário de destino.

A ousadia dos autores é tão grande que
o título do e-mail faz sentido e o texto condiz
com o trabalho diário. Se não ficar atento, cai no golpe.



Não abra emails ou clique em links de mensagens com conteúdo estranho
que não condiz com o trabalho diário, ou que contenha no cabeçalho um endereço estranho.

EXEMPLO DE ATAQUE PHISHING

De: Departamento financeiro
Enviada em: sexta-feira, 25 de março de 2022 09:12
Para:
Assunto: Message has been processed :ATENCAO! Mensagem Importante! - id - (464398)

NOTIFICAÇÃO EXTRAJUDICIAL

Atenção!

BOM DIA (A)!

Apesar das oportunidades oferecidas pel
regularização da sua pendência, observamo
liquidação do débito.. Por este motivo, **inform**
do nome.

Solicitamos que entre em contato no **pr**
horas para a realização de um acordo
favoráveis.

http://http.masassistenkiwertgt.com/DocBr2?
upn=O2sw8NkhhRVChOFX-2B5RdlD0cTxG-2F1bRAPu
6OxaNPFbZd2sF0042LqeRE9HnYMxKiYIfC_mSdDBA
W1x88ry1ia-2BQGEI2oQA93LTUAYe4qcgKpqWBxlh-2
Fy70tCHKYe-2FB3f9-2BVfpkjHmKoWOms0wYGujl2XE
6qpghehwBxHKt11wgppehOxyTNPV6oAhwgZ-2FsDGw
13FFxAoMVmw5VboDSYj09v6eRU6dUtOd-2FwbcMfa
0u9oLYU3VFcmbK3ubw2tNo3nvCmFX2EMFxrkyfdcxZ
T6HbyV2Dgi54x173cEo9wEDbMUpYGWJIZNXJOOHOf
b44KNu4u6UgD48NHchocPq-2Fil2kN95qCwZXPiHOk
orcQKdEZNpsCE-2BNb8iF7UNnrFXUZzSg7Nnva44qa
Yf6am8ufZJvac6bA-3D-3D

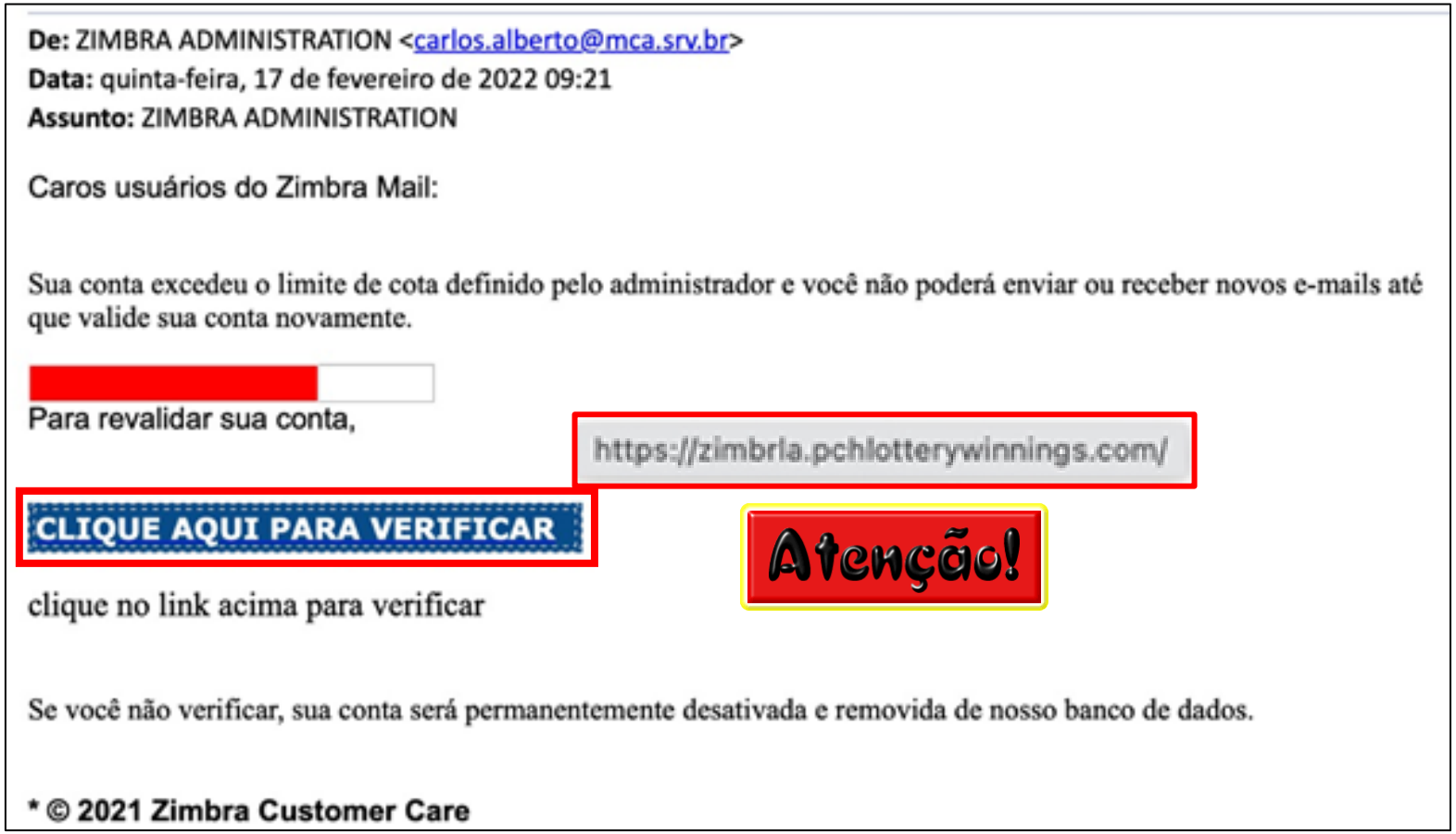
Consultar Extrato de Débitos aqui!

E-mail automático. Por favor, não responda.

EXEMPLO DE ATAQUE PHISHING

Este outro e-mail parece normal?

Até então parece algo enviado pela TI ou enviado automaticamente pelo servidor de e-mail informando que necessita validar sua conta de e-mail.



De: ZIMBRA ADMINISTRATION <carlos.alberto@mca.srv.br>
Data: quinta-feira, 17 de fevereiro de 2022 09:21
Assunto: ZIMBRA ADMINISTRATION

Caros usuários do Zimbra Mail:

Sua conta excedeu o limite de cota definido pelo administrador e você não poderá enviar ou receber novos e-mails até que valide sua conta novamente.

Para revalidar sua conta,

https://zimbrla.pchlotterywinnings.com/

CLIQUE AQUI PARA VERIFICAR

Atenção!

clique no link acima para verificar

Se você não verificar, sua conta será permanentemente desativada e removida de nosso banco de dados.

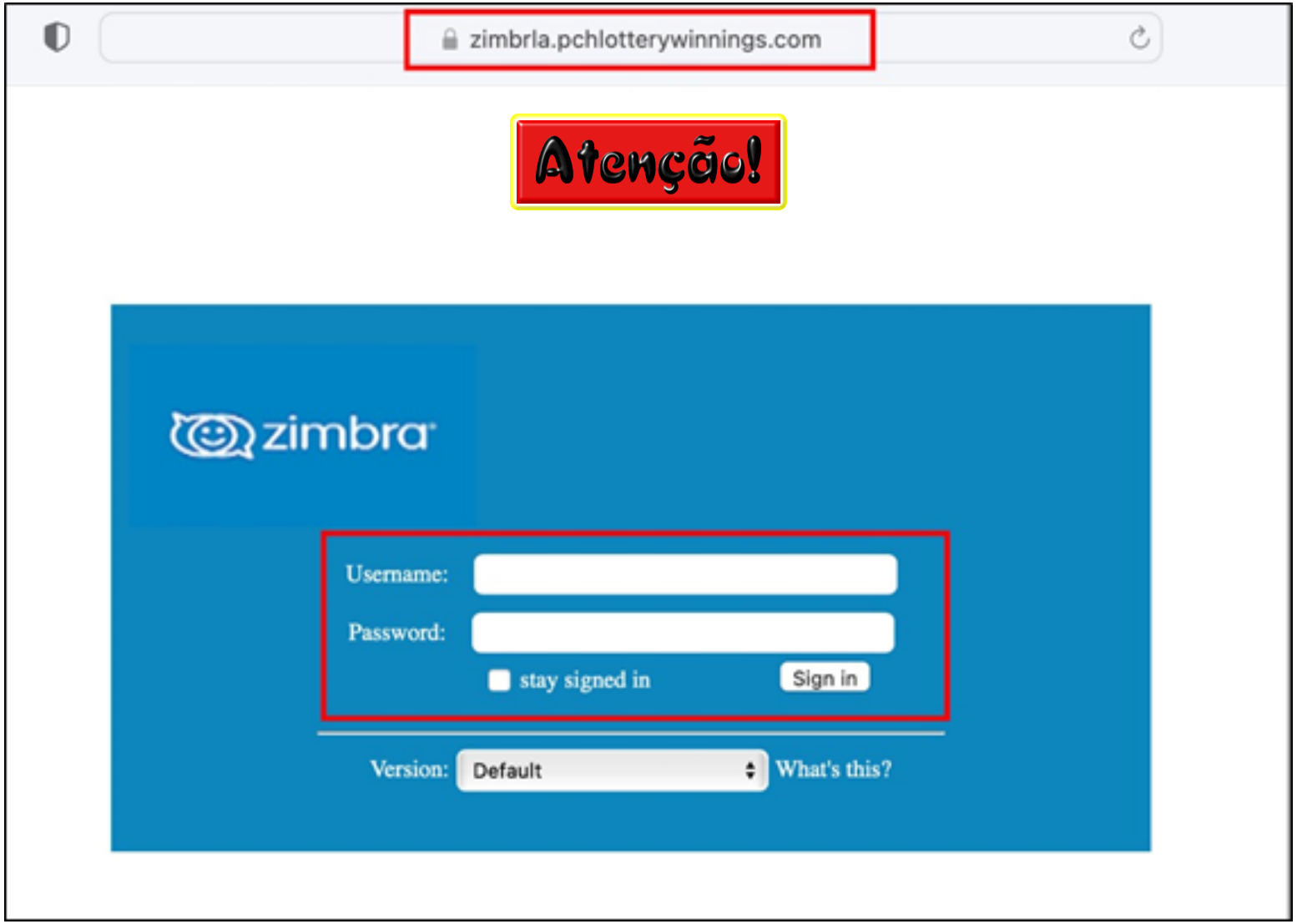
* © 2021 Zimbra Customer Care

EXEMPLO DE ATAQUE PHISHING

Ao clicar no link irá abrir uma página para inserir o e-mail e sua senha. Isso é um golpe!

Aqui os golpistas terão acesso ao seu e-mail e sua senha.

Jamais repasse suas senhas para alguém, elas são pessoais e intransferíveis.



OBRIGADO!

ALLAN KOVALSCKI
DIRETOR GERAL

+55 51 9 9988.5350

allan.kovalscki@complylgpd.com.br

www.complylgpd.com.br

Tv. Francisco de Leonardo Truda, 98 - 6º andar - Centro Histórico, Porto Alegre

COMPLY LGPD SOLUTIONS