MailSecurity Protection.

Parabéns! Você deu um grande passo para combater a fraude de e-mail.

Iniciação ao DMARC

mailsecurity.com.br

E-BOOK

Introdução

US$ 26,2 bilhões

foi quanto o BEC custou a organizações do mundo todo desde 2016 (fonte: FBI)

US$ 157.000

foi o custo líquido por incidente de um ataque de BEC global médio (fonte: FBI)

473%

foi o aumento em tentativas de fraude de e-mail contra organizações visadas no quarto trimestre de 2018 em relação ao mesmo trimestre do ano anterior (fonte: Proofpoint)

86%

das organizações afirmaram ter sofrido ataques de phishing em 2019, um aumento de 83% em relação a 2018 (fonte: relatório State of the Phish da Proofpoint)

O e-mail é excelente para negócios: é barato, expansível e, o mais importante, eficaz em promover leads e receita. Infelizmente, as mesmas coisas que tornam o e-mail tão popular — facilidade de uso, conveniência, transparência — também fazem dele um vetor preferencial para cibercriminosos.

A fraude de e-mail custa bilhões a empresas do mundo todo e pode destruir a reputação da marca e a confiança do consumidor em questão de minutos. Golpes de comprometimento de e-mail corporativo (BEC) de baixo volume e altamente direcionados são considerados os mais perigosos, tendo custado a organizações do mundo todo US$ 26,2 bilhões desde 2016, segundo o FBI.

O padrão **DMARC**, lançado por um grupo de organizações líderes em e-mail em fevereiro de 2012, é uma das armas mais poderosas e proativas já criadas para combater phishing e falsificação.

Ele remodelou o cenário de fraudes de e-mail, atingindo estratégias de phishing de longa data e obrigando os criminosos cibernéticos a abandonar seus alvos preferidos. O DMARC tem o potencial de anular uma classe inteira de fraudes nos próximos anos.

Neste guia, abordaremos o que é o DMARC, como funciona, suas principais vantagens e porque ele deve ser uma parte fundamental das suas defesas contra BEC e EAC.

O atue é DMARC?

Lançado em 2012 por um consórcio do setor, o DMARC — Domain-based Message Authentication Reporting and Conformance — é um protocolo aberto de autenticação de e-mail que possibilita a proteção do canal de e-mail em nível de domínio.

Criado com base nos padrões SPF e DKIM já existentes, o DMARC é a primeira e única tecnologia amplamente distribuída que pode tornar confiável o domínio do cabeçalho de remetente (que os usuários veem em seus programas de e-mail).

DMARC

Domain-based

Message

Authentication

Reporting &

Conformance

- Padrão aberto de autenticação de e-mail
- Lançado em 2012
- Fundado por mais de 20 empresas

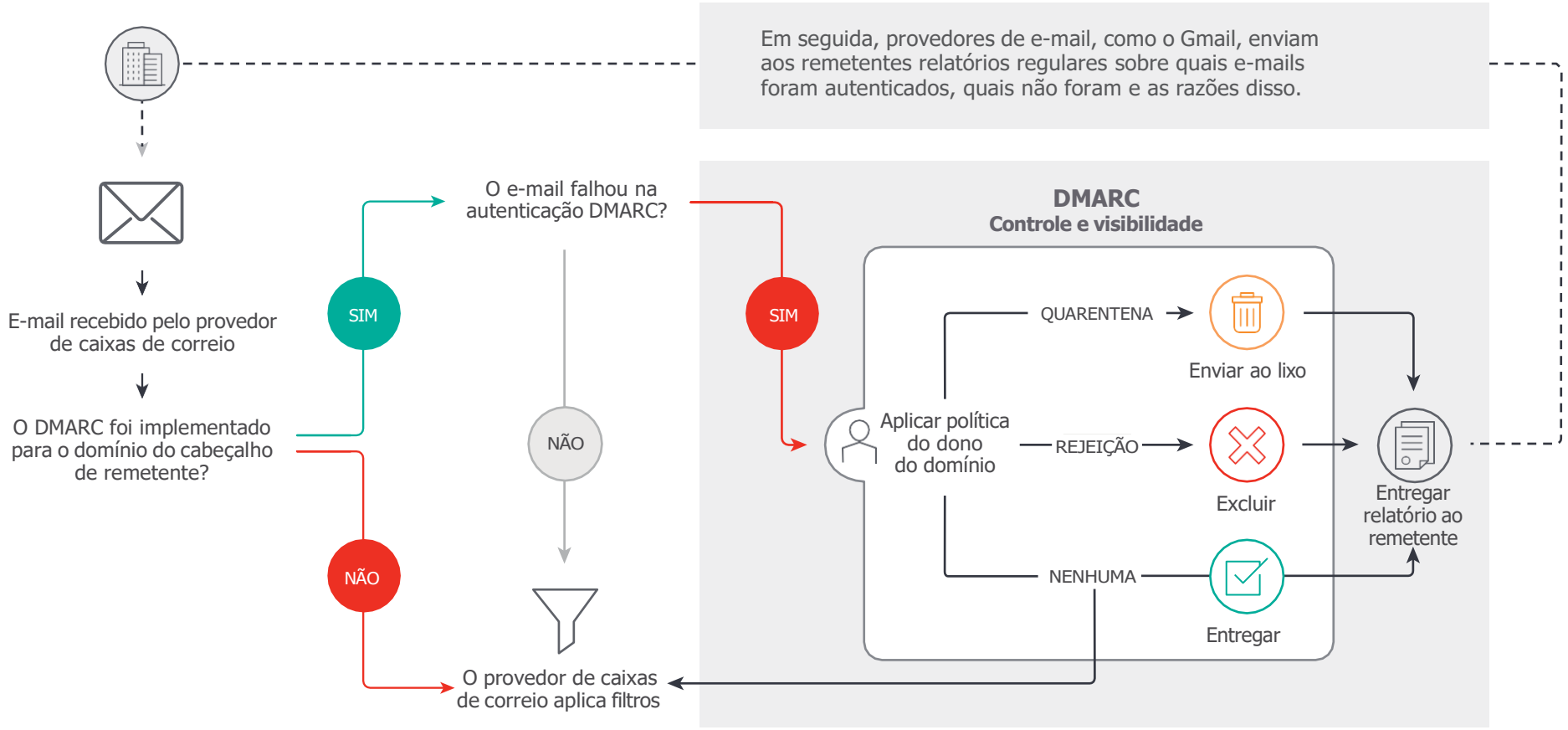
O DMARC permite aos remetentes de e-mail:

Reaver o controle autenticando mensagens de e-mail legítimas em seus domínios de envio de e-mail.

Informar aos provedores de caixas de correio como tratar as mensagens que não passarem na autenticação, através de uma configuração de política explícita. Essas mensagens podem ser enviadas para uma pasta de lixo ou simplesmente rejeitadas, protegendo consumidores contra exposição a ataques.

Obter insights sobre o cenário de ameaças de e-mail para ajudá-lo a identificar ameaças contra os seus clientes e proteger melhor a sua marca contra phishing e falsificação.

Como funciona o DMARC



Configurações de política DMARC

Nenhuma: Todo o ecossistema de autenticação de e-mail é monitorado para mapear o tráfego legítimo.

Quarentena: Mensagens que não satisfazem o DMARC são movidas para a pasta de spam.

Rejeição: Mensagens que não satisfazem o DMARC não são entregues.

Por atue DMARC?

O DMARC capacita os remetentes a:

- Obter visibilidade sobre quem está enviando em seu nome, quais e-mails estão sendo autenticados, quais não estão e as razões disso.
- Informar aos destinatários dos e-mails como tratar os e-mails que não passarem na autenticação.
- Bloquear ataques de phishing que falsifiquem domínios pertencentes ao remetente, antes que cheguem às caixas de entrada de funcionários e consumidores.

O DMARC capacita os destinatários a:

- Diferenciar remetentes legítimos de remetentes maliciosos.
- Promover a lealdade do consumidor e a proteção dos funcionários.
- Melhorar e proteger a reputação do canal de e-mail.

"O padrão DMARC simplesmente funciona. Com uma abordagem mista para combater a fraude de e-mail, o DMARC representa a pedra angular dos controles técnicos... para reconstruir a confiança e resgatar o canal de e-mail para marcas e consumidores legítimos."

Edward Tucker, chefe de segurança cibernética do HM Revenue & Customs do Reino Unido

"Com políticas DMARC mais rigorosas, os usuários ficam mais seguros e os malfeitores ficam em uma saia justa. O mais importante é que remetentes verificados têm acesso a uma enorme onda de inovação e avanço para todas as nossas caixas de entrada."

Jeff Bonforte, vice-presidente sênior de produtos de comunicação da Yahoo!

As vantagens do DMARC

Protege funcionários, parceiros comerciais e consumidores.	O DMARC elimina uma classe inteira de e-mails fraudulentos antes que estes cheguem aos seus funcionários, parceiros e consumidores.
Oferece insights imediatos sobre o cenários de ameaças de e-mail.	Não se controla o que não se vê! A implementação do DMARC proporciona visibilidade instantânea sobre as ameaças que visam a sua empresa. Efetivamente, ele lança luz sobre ataques de falsificação e phishing de domínio que colocam em risco a reputação da sua marca e seus consumidores.
Aumenta a entregabilidade e o engajamento do e-mail.	Aproximadamente um em cada cinco ataques de phishing resulta em redução da entregabilidade e um em cada três resulta em redução do engajamento do e-mail. O DMARC aumenta tanto a entregabilidade quanto o engajamento de programas de e-mail legítimos.
Reduz os custos de atendimento ao consumidor.	Ao bloquear ataques de phishing, o DMARC reduz consideravelmente os custos de atendimento ao consumidor. A rede varejista Blocket, da Escandinávia, teve uma queda de 70% nos tíquetes de atendimento ao consumidor após implementar o DMARC.
Reduz os custos de remediação de phishing.	O phishing custa às marcas US$ 4,5 bilhões por ano. O DMARC reduz os gastos com fraudes, reembolso e remediação de phishing.

DMARC em números

86%
das caixas de correio de consumidores globais têm o DMARC ativado.

32%
das organizações Global 2000 adotaram a autenticação DMARC

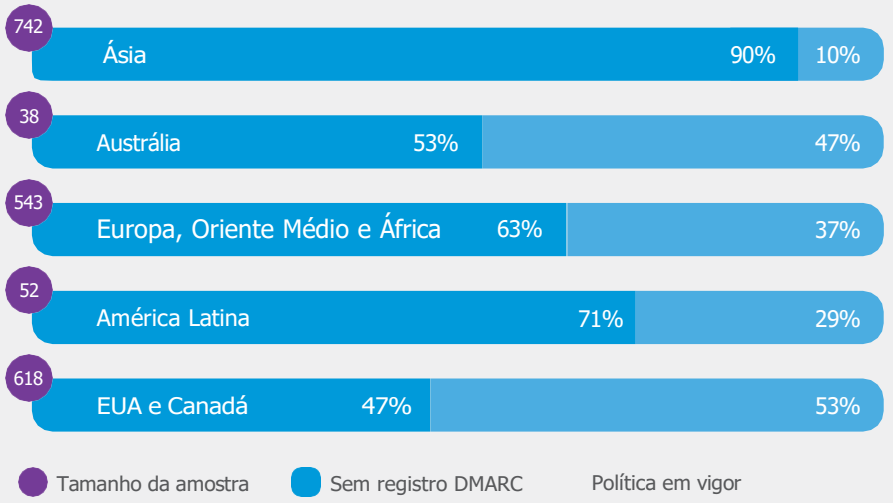
6%
das organizações Global 2000 implementaram uma política DMARC de rejeição

Adoção do DMARC por setor em 2019

SEGMENTO	TAMANHO DA AMOSTRA	ADOÇÃO DO DMARC
Tecnologia	94	59%
Saúde	33	58%
Seguros	56	41%
Varejo	88	41%
Farmacêutico	29	38%
Serviços financeiros	524	34%
Transportes	64	33%
Manufatura	219	32%
Energia/serviços públicos	175	29%
Telecomunicações	48	29%
Construção civil	55	20%
Automotivo	49	18%
Imobiliário	53	13%

Amostra: Organizações Global 2000

Crescimento da adoção global do DMARC por remetentes em 2019



Amostra: Organizações Global 2000

Fonte: DMARC

Autenticação de e-mail em revista

O DMARC foi criado com base em dois outros padrões de autenticação de e-mail extremamente importantes: o SPF (Sender Policy Framework) e o DKIM (DomainKeys Identified Mail). Para entender completamente o DMARC, você também precisa compreender as vantagens do SPF e do DKIM — e suas limitações.

	SPF	DKIM	DMARC
	(Sender Policy Framework) www.open-spf.org	(DomainKeys Identified Mail) www.dkim.org	(Domain-based Message Authentication Reporting & Conformance) www.dmarc.org
Vantagens	O SPF permite que as marcas especifiquem quem pode enviar e-mails em nome de seu domínio. As marcas listam os endereços IP dos remetentes autorizados em um registro de DNS. Se o endereço IP que estiver enviando e-mail no nome da marca não estiver listado naquele registro SPF, a mensagem não passará na autenticação SPF.	O DKIM permite que uma organização se responsabilize pela transmissão de uma mensagem de uma maneira que pode ser verificada pelo provedor de e-mail. Essa verificação é possibilitada por uma autenticação criptográfica dentro da assinatura digital do e-mail.	O DMARC assegura que o e-mail legítimo seja devidamente autenticado conforme os padrões estabelecidos DKIM e SPF e que atividades fraudulentas que aparentem se originar de domínios sob controle de uma marca sejam bloqueadas antes de chegar à caixa de entrada do consumidor.
Exemplo de registro de DNS	v=spf1 ip4:204.200.197.197 -all	v=DKIM1; p=MIGfMA0GCSqGSIb3DQEBAQUAA4G NADCBiQKBgQDfl0chtL4siFYCrSPxw43fqc4z Oo3N	v=DMARC1; p=reject; fo=1; rua=mailto:dmarc_ agg@auth.yourdomain.com;ruf=mailto:dmarc_ afrf@auth.yourdomain.com
Falhas	• É difícil manter atualizados os registros SPF enquanto as marcas trocam de provedores de serviços e acrescentam fluxos de e-mail. • Só porque uma mensagem não passa no SPF, isso não significa que ela será sempre impedida de chegar à caixa de entrada. • O SPF falha quando uma mensagem é encaminhada. • O SPF não faz coisa alguma para proteger marcas contra criminosos cibernéticos que falsificam o nome de exibição ou o endereço do cabeçalho de remetente da mensagem.	• O DKIM é mais difícil de implementar e, por isso, menos remetentes o adotam. • Essa adoção inconsistente significa que a ausência de uma assinatura DKIM não indica que o e-mail é necessariamente fraudulento. • O DKIM, isoladamente, não é uma maneira universalmente confiável de autenticar a identidade de um remetente. • O domínio DKIM não é visível para o usuário final leigo e nada faz para evitar a falsificação do domínio visível do cabeçalho de remetente.	• Embora essencial, o DMARC não é uma solução completa. • O DMARC só protege a sua marca contra 30% dos ataques de e-mail (ameaças diretas ao domínio). • O DMARC não protege contra falsificação da marca (o que inclui falsificação do nome de exibição e uso de domínios parecidos).

Campeões do DMARC – marcas

Esses campeões do DMARC abriram o caminho para a criação do padrão. Esses precursores estão na vanguarda da luta contra a fraude de e-mail e estão defendendo proativamente seus clientes contra criminosos cibernéticos.

"Ao longo dos últimos anos, cada vez mais empresas vêm adotando o DMARC e a autenticação de e-mail e mais fornecedores e provedores de serviços estão acrescentando às suas ofertas o suporte necessário para simplificar a adoção."

Steven Jones, DMARC.org

"Após implementar uma política DMARC de rejeição, vimos os tíquetes de atendimento ao consumidor caírem mais de 70%, significando que a equipe de atendimento pôde se concentrar em atender consumidores em consultas geradoras de receita."

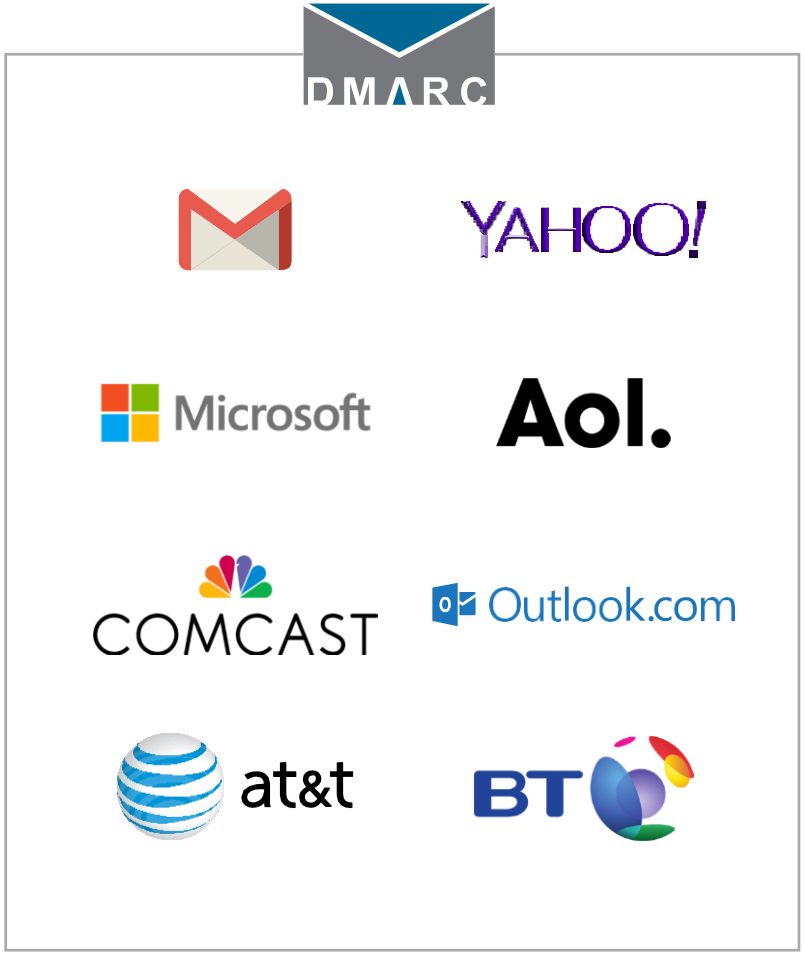
Thomas Bäcker,
chefe de segurança do consumidor da Blocket

Campeões do DMARC – provedores de caixas de correio

Alguns dos maiores provedores de caixas de correio do mundo estão apoiando o DMARC. Estima-se hoje que 70% das caixas de entrada de consumidores do mundo são protegidas pelo DMARC.

"Estamos avançando rapidamente para um mundo no qual todo e-mail será autenticado. A implementação de uma política DMARC assegura que a reputação do remetente não seja prejudicada devido às ações dos fraudadores. Se o seu domínio não se protege com o DMARC, as chances serão maiores de que as suas mensagens sejam enviadas diretamente para uma pasta de spam ou até mesmo rejeitadas."

John Rae-Grant,
gerente de produto da Google



"Da noite para o dia, os malfeitores que utilizavam falsificação de e-mail para forjar e-mails e iniciar tentativas de phishing aparentemente originadas de uma conta do Yahoo! Mail foram bloqueados sumariamente."

Jeff Bonforte, vice-presidente sênior de produtos de comunicação da Yahoo!

Glossário de tags DMARC

As tags DMARC são a linguagem do padrão DMARC. Elas dizem ao recebedor do e-mail que verifique se há DMARC e informam o que fazer com as mensagens que não passam na autenticação. Para obter mais informações sobre todas as tags DMARC, clique aqui.

Nome da tag	Obrigatória?	Finalidade	Exemplo
v	Sim	Versão do protocolo	v=DMARC1
p	Sim	Política de domínio	p=quarantine
pct	Opcional	% das mensagens sujeitas a filtragem	pct=20
rua	Opcional	URI de relatórios agregados	rua=mailto:aggrep@exemplo.com
sp	Opcional	Política para subdomínios do domínio	sp=reject
aspf	Opcional	Modo de alinhamento para SPF (estrito ou relaxado)	aspf=r
ruf	Opcional	URI de relatórios forenses	ruf=mailto:aggrep@exemplo.com
adkim	Opcional	Alinhamento para DKIM (estrito ou relaxado)	adkim=r
ri	Opcional	O número de segundos decorridos entre o envio de relatórios agregados ao remetente	ri=86400
fo	Opcional	Oferece opções para geração de relatórios de falha	"fo=1"

Hora de iniciar sua jornada DMARC

O BEC e seu parente próximo, o comprometimento de contas de e-mail (EAC), são complexos e multifacetados. Por isso que eles exigem uma solução completa que lide com todas as táticas dos atacantes — e não apenas algumas.

Embora não exista bala de prata contra BEC e EAC, a distribuição do DMARC é um bom começo. Trata-se de um componente fundamental na defesa contra ameaças de impostura, especialmente as que falsificam domínios de e-mail confiáveis. O DMARC é a maneira mais eficaz de proteger contra falsificação de domínio e de impedir que e-mails fraudulentos utilizem o seu domínio.

Nós, da MailSecurity, ajudamos algumas das maiores marcas do Brasil a distribuir o DMARC com êxito. Embora cada organização seja um caso, a maioria segue estes passos para distribuição completa ao longo do tempo.

Tudo começa com um primeiro passo muito simples: criar um registro DMARC no DNS e lançar luz sobre todo o seu ecossistema de e-mail.

Passo 1

Selecione um domínio.

(Este pode ser o seu domínio de nível mais alto ou um subdomínio que envie muito e-mail)

Passo 2

Gere o seu registro utilizando nosso **Assistente de criação de DMARC.** (Especifique a política do recebedor de e-mail como "nenhuma")

Passo 3

Colabore com o seu administrador de servidores para adicionar o seu registro DMARC ao DNS.

Passo 4

Comece a receber relatórios DMARC sobre o seu domínio.

Passo 5

Entre em contato com nossa equipe de fraudes para que o ajudemos a entender rapidamente o seu ecossistema de e-mail.

Parabéns! Você deu um grande passo para combater a fraude de e-mail.

Para saber mais sobre como a MailSecurity pode ajudá-lo a combater efetivamente ataques de BEC/EAC, confira nosso resumo de solução *"https://mailsecurity.com.br/mailsecurity-dmarc/"* (Sete maneiras de se defender contra BEC e EAC com a MailSecurity)

SAIBA MAIS

Para obter mais informações, visite
mailsecurity.com.br

SOBRE A MAIL SECURITY

A MAILSECURITY é uma empresa especialista em segurança de emails corporativos e cibersegurança que protege as organizações em seus maiores riscos e seus ativos mais valiosos. Com emails corporativos integrado com soluções de segurança de emails avançada baseadas em nuvem, a MailSecurity ajuda empresas de todo o Brasil a deter ameaças direcionadas a seus emails corporativos, proteger seus dados e tornar seus usuários mais resilientes contra ataques cibernéticos. Nossos parceiros são organizações líderes de todos os portes, incluindo 75% das empresas da Fortune 100, fazem parceria com a MailSecurity para fornecer soluções de segurança e conformidade centradas nas pessoas e que minimizem seus riscos mais críticos em e-mail corporativos, nuvem, redes sociais e Web. Mais informações estão disponíveis em www.mailsecurity.com.br.

0503-003-01-01 08/20