

# MANUAL DE COMPORTAMENTO DIGITAL SEGURO



**RIOgaleão**  
aeroporto  
internacional  
tom jobim



## BEM-VINDO À FAMÍLIA RIOGALEÃO!

**A Tecnologia da Informação (TI) está cada vez mais presente em nossas vidas.** Profissionais passam a ser filiais móveis, carregando consigo equipamentos de conexão, uso e acesso a informações corporativas, muitas delas sigilosas por motivos de propriedade intelectual, de diferencial competitivo ou por razões legais.

**Este manual apresenta uma introdução ao tema de Segurança da Informação,** com orientações de segurança a serem utilizadas tanto em sua vida pessoal, quanto em sua vida corporativa. **As Políticas de Segurança da Informação do RIOgaleão devem ser lidas por todos os integrantes.** Elas se encontram na [biblioteca de documentos](#) existente no [Portal Conexão](#).



E lembre-se: a tecnologia ajuda (e muito), mas não faz o nosso trabalho e nem garante a nossa segurança. **A Segurança da Informação é responsabilidade de cada Integrante.**

# ÍNDICE

Os dados que você compartilha diariamente estão protegidos? .....03

O que é Segurança da Informação?

Credenciais .....04

Como criar senhas fortes? .....05

Você sabe o que é verificação em duas etapas?

Engenharia social .....06

Tipos de Engenharia Social

Mas qual o perigo do phishing? .....07

Invasão Física .....08

Identidade Pessoal x Identidade Corporativa

Reconhecendo sites seguros .....09

Além do HTTPS

# Os dados que você compartilha diariamente estão protegidos?

Atualmente, trocamos informações a todo momento, por meio de serviços de mensagens, aplicativos de locomoção, delivery e bancos.

**Mas fique atento!** Da mesma forma que é fácil termos acesso a tudo que está na internet, é fácil também para os ciberatacantes encontrarem brechas de segurança para roubar nossos dados.

Para apoiar o seu conhecimento, desenvolvemos este guia na qual você aprenderá boas práticas para garantir a segurança de seus dados e do RIOgaleão!

**Não deixe de conferir!**

## O que é Segurança da Informação?

A Segurança da Informação cuida da proteção de dados em todas as suas formas, seguindo 3 pilares conhecidos como CID (Confidencialidade, Integridade e Disponibilidade).

**Confidencialidade:** Garante que somente pessoas autorizadas tenham acesso às informações, como usuário e senha (que são pessoais e intransferíveis).

**Integridade:** Garante que as informações utilizadas pelos processos de negócio e com as quais trabalhamos todos os dias estejam sempre completas e corretas.

**Disponibilidade:** Garante que as informações e os recursos de tecnologia que utilizamos no dia a dia (nossos equipamentos, rede corporativa etc.) estejam disponíveis sempre que necessários.

Com a aplicação diária do conceito CID em cada atividade, as informações serão acessadas e manipuladas somente por pessoas autorizadas, garantindo a segurança e disponibilidade dos dados para a utilização pelos usuários que tiverem permissão.

Uma segurança efetiva só é conquistada com a participação e apoio de todos. Falhas humanas acontecem e predominam como causa principal na maioria dos eventos de segurança.

A colaboração de todos é essencial nessa jornada e juntos estamos mais protegidos.

É preciso estar atento o tempo todo, seja com nossas credenciais, senhas ou com nossa navegação na Internet. Ao diminuir nossos erros, aumentamos nossa proteção.

## Credenciais

Credencial é tudo aquilo que é utilizado para nos identificar, podendo ser um crachá, um RG, CPF e até uma carteira de conselho profissional (CREA, CREMERJ).

Logins e senhas são a forma de credencial mais utilizada em TI, comumente reforçada com o uso de outras tecnologias para criar múltiplas confirmações de sua Identidade Digital (ex.: Token digital ou aprovação via celular).

### Já pensou no perigo se um estranho tivesse uma cópia da chave da sua casa?

Isso é o que acontece quando você divide sua senha com outras pessoas. Por isso:

- Não compartilhe suas senhas, nem as anote em agendas ou post-its;
- Não utilize nomes ou partes dos nomes do RIOgaleão (RIOgaleao@2017);
- Não utilize combinações com dados pessoais (CEduardo@1982);
- Não usar a mesma senha para assuntos pessoais e corporativos. Não misture sua identidade pessoal com sua identidade corporativa;
- Altere a senha com frequência (na frequência requerida pelas políticas de segurança da informação do RIOgaleão ou sempre que for solicitado).

**Viu como precisamos de você  
para garantir a segurança das  
informações do RIOgaleão?**



## Como criar senhas fortes?

Você está se perguntando como irá criar uma senha longa, difícil de se adivinhar e relativamente fácil de se lembrar, certo?

**É simples, veja só!**

- Escolha uma frase que você lembre com facilidade e que faça sentido para você. Ex: “Água Mole em Pedra Dura Tanto Bate até que Fura”
- Pegue a primeira letra de cada palavra da frase: AMEPDTBAQF
- Acrescente símbolos e números, letras maiúsculas e minúsculas: 4m3pd@tbaqF

**Incrível, né!**

**E não se esqueça:**

- Nada de reprise! Não repita senhas já utilizadas;
- Pense grande, construa uma senha com 10 ou mais caracteres;
- Sempre use letras maiúsculas, letras minúsculas, números e símbolos (todas estas opções ao mesmo tempo!) ao construir sua senha
- E se a senha for numérica? Crie uma ordem aleatória (ex: os números do prédio e apartamento de algum amigo da época de colégio ou um número de telefone antigo de uma pessoa não próxima)



## Você sabe o que é verificação em duas etapas? É bem fácil!

A dupla autenticação é uma camada adicional de proteção no momento do login de serviços e contas digitais. Além da sua senha, será solicitado um segundo código de verificação, que pode ser por um código numérico, biometria ou autorização de acesso de software (responder sim ou não a uma solicitação de login) por meio de outro dispositivo.

O RIOgaleão está sempre trabalhando para oferecer uma autenticação mais segura para seus integrantes, utilizando as melhores tecnologias e observando a legislação existente e as determinações de órgãos reguladores (ANAC, Receita Federal etc.).

**#Fica a Dica!**

**No caso de suas identidades digitais pessoais, você é seu próprio legislador e regulador!** Vá em frente e habilite o duplo fator de autenticação sempre que possível – no Google, Microsoft, Facebook, Twitter, WhatsApp, Telegram, entre outros. **É muito simples e você ficará ainda mais seguro!**

## Engenharia social

Engenharia Social é o nome dado a golpes que precisam da ação da vítima para terem sucesso. Ou seja, para o criminoso conseguir acessar uma conta, ele precisa antes que a pessoa informe seus dados, por exemplo.

### Tipos de Engenharia Social

Existem diversos tipos de ameaças envolvendo engenharia social, tanto no meio digital quanto no ambiente físico. Os golpes podem vir:

- Por meio de mensagens falsas enviadas por e-mail e apps de mensagem;
- Através de mensagens falsas enviadas por SMS;
- Por meio de golpes telefônicos (os tão conhecidos trotes);
- Golpes com mídias removíveis infectadas com vírus;
- Invasão física (carona em catracas).

#### **CUIDADO COM MENSAGENS FALSAS (PHISHINGS)!**

O phishing é o ataque de engenharia social mais comum. Os ciberatacantes costumam enviar mensagens falsas (phishings) por e-mails, chats ou aplicativos, com links ou arquivos maliciosos para fisgar suas vítimas e roubar dados!



## Mas qual o perigo do phishing?

- Roubo/vazamento das informações de computadores ou celulares;
- Contaminação de diversas máquinas e o controle delas;
- Sequestro de dados de uma pessoa ou equipamento, cobrando pelo resgate;
- Espionagem de tudo o que acontece no dispositivo.

## Recebeu um e-mail?

- Verifique se você conhece quem te enviou a mensagem;
- Se o conteúdo da mensagem possuir muitos erros gramaticais, desconfie;
- Não clique em links por conta do tom de urgência usado na mensagem, por exemplo, "Participe agora!".
- Suspeite ao receber e-mails com o nome de contato de um conhecido, mas com um conteúdo completamente diferente do que você costuma receber da pessoa, mesmo que seja seu gerente ou diretor. Sempre verifique se o domínio do e-mail está correto.
- Cuidado com e-mails de pessoas que dizem ser gerentes, diretores, delegados da polícia federal, fiscais da receita. Ciberatacantes usam de títulos importantes para que você não conteste a veracidade da mensagem.

**Em caso de qualquer suspeita, confirme sempre a validade com seu gestor e caso a suspeita se concretize, encaminhe o e-mail para [securityti@riogaleao.com](mailto:securityti@riogaleao.com) (r. 4911) para bloqueio de futuros e-mails do mesmo tipo e demais providências.**

## Invasão Física

As ameaças não são particularidades do mundo digital, também acontecem em ambientes físicos.

Antes de acessar as dependências da empresa, fique atento se não há pessoas esperando para “pegar carona” com você. Essa prática acontece em catracas, elevadores e portas com abertura automática, possibilitando que terceiros consigam acesso a ambientes físicos sem autorização.

**Além disso, não empreste seu crachá para que outros acessem as dependências do RIOgaleão, isso não é permitido.**



**Caso veja isso acontecendo com você ou com algum colega, procure a equipe de Segurança da Informação.**

## Identidade Pessoal x Identidade Corporativa

Com uma vida cada vez mais conectada, nossa atenção deve ser constante para não misturarmos recursos pessoais e corporativos. **Por isso, ressaltamos!**

A utilização de contas pessoais de e-mail e redes sociais, contas pessoais de WhatsApp, Telegram e outros aplicativos similares, para tratar de assuntos de trabalho não é permitida em qualquer hipótese! O contrário também é verdade. Nunca utilize contas, redes e canais corporativos para tratar de assuntos pessoais!”

### Exemplos de uso pessoal de recursos corporativos

- Utilização do número de celular corporativo para participação em grupos pessoais de WhatsApp, Telegram etc;
- Utilização de e-mail corporativo ou identidade corporativa para inscrição em fóruns, redes sociais, listas de distribuição, e-commerces etc.
- Uso de ferramentas corporativas para enviar conteúdo, fotos ou vídeos que não tenham relação com seu trabalho.

## Reconhecendo sites seguros

Fazer com que usuários acessem sites falsos também é uma forma de phishing. Saiba como reconhecer um site falso.

O protocolo HTTPS é identificado por um cadeado junto ao endereço do site no seu navegador.

**É importante lembrar que o HTTPS não significa que o site é seguro, pois ele não certifica o conteúdo, apenas sinaliza que o tráfego entre você e o servidor está “protegido” contra visualização indevida.**

### Além do HTTPS:

Seu navegador emite qualquer mensagem do tipo “Certificado não válido” ou, mais explicitamente, “Site não confiável” – nunca acesse sites deste tipo, pois eles podem instalar malwares em seu equipamento;

- O navegador não emite qualquer mensagem, mas o domínio é diferente: <https://tracking.rgaleao.online/> ao invés de <https://tracking.riogaleao.com/>
- Não entre em sites que só liberam o acesso após você fornecer seus dados pessoais. Você deve ter a escolha se quer ou não efetuar um cadastro.

### Troca de informações com terceiros

A correta proteção da informação é ainda mais crítica nas interações com terceiros. Em caso de informações sensíveis procure:

- Certificar se o destinatário está correto ao enviar mensagens, seja por e-mail, SMS e WhatsApp por celular corporativo;
- Compartilhar arquivos sensíveis somente após autorização da área jurídica. Mesmo havendo um acordo de não-divulgação assinado pelas partes;
- Proteger as informações com senha e enviar o código de acesso por outro canal. Envie, por exemplo, o arquivo por e-mail e a senha por WhatsApp corporativo.

Em caso de dúvidas, entre em contato com o setor de Segurança da Informação, por meio dos seguintes canais:

**e-mail: [securityti@riogaleao.com](mailto:securityti@riogaleao.com)**  
**Telefone: (21) 3721-4911**

**Contamos com você, a Segurança da Informação é uma  
responsabilidade de todos nós!**

