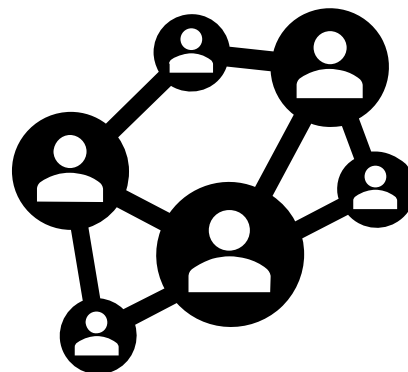


## GUIA DE RECOMENDAÇÕES PARA TRABALHO REMOTO SEGURO

Prezados,

Apresentamos recomendações e orientações IMPORTANTES da CGTI quanto às ameaças diversas na internet, uma vez que, a estação pessoal do usuário se torna uma parte da rede do IPHAN.

A **segurança da informação é responsabilidade de todos os usuários**, um ponto fraco pode comprometer toda a informação.



### Recomendamos:

- ♦ Utilizar um bom **antivírus** nas estações pessoais, de preferência ferramentas licenciadas com vacinas atualizadas diariamente, e ative o **firewall** do Windows;
- ♦ Não salvar senhas nos navegadores (função lembrar-me);
- ♦ Baixar os arquivos e trabalhar offline (desconectar da página web); se necessário, depois de editar, subir via FTPs;
- ♦ Outros acessos à internet não devem ser realizados quando conectados ao IPHAN;
- ♦ Evitar que o acesso ao IPHAN seja feito a partir de computadores públicos e não confiáveis;
- ♦ Não utilizar pen-drives e HDs externos quando estiverem conectados ao IPHAN.

### Alguns cuidados para proteção contra golpes na internet:

- ♦ Fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links;
- ♦ Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança);
- ♦ Fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;
- ♦ Não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada seja cuidadoso ao acessar links. Procure digitar o endereço diretamente no navegador Web;
- ♦ Verifique o link apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o link real para o *phishing*. Ao posicionar o mouse sobre o link, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;
- ♦ Acesse a página da instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).




Caso necessite de mais informações entre em contato com a central de atendimento ao usuário do IPHAN pelo telefone **0800 940 1210** ou através do OTRS <http://centraldeservicos.iphan.gov.br/> .

## Orientações para senhas:




**Não forneça as suas senhas para outra pessoa, em hipótese alguma;  
Troque sempre que achar necessário, antes mesmo da política de reset de senha.**

*Uma senha boa, bem elaborada, é aquela que é **difícil de ser descoberta (forte) e fácil de ser lembrada.**  
Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la.  
Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante.*




Alguns elementos que você **DEVE** usar na elaboração de suas senhas são:

-  Números aleatórios: quanto mais ao acaso forem os números usados melhor, principalmente em sistemas que aceitem exclusivamente caracteres numéricos;
-  Grande quantidade de caracteres: quanto mais longa for a senha mais difícil será descobri-la. Apesar de senhas longas parecerem, a princípio, difíceis de serem digitadas, com o uso frequente elas acabam sendo digitadas facilmente;
-  Diferentes tipos de caracteres: quanto mais "bagunçada" for a senha mais difícil será descobri-la. Procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas. O uso de sinais de pontuação pode dificultar bastante que a senha seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

Alguns elementos que você **NÃO DEVE** usar na elaboração de suas senhas são:

-  Qualquer tipo de dado pessoal: evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas (estes dados podem ser facilmente obtidos e usados por pessoas que queiram tentar se autenticar como você);
-  Sequências de teclado: evite senhas associadas à proximidade entre os caracteres no teclado, como "1qaz2wsx" e "QwerTAsdfG", pois são bastante conhecidas e podem ser facilmente observadas ao serem digitadas;
-  Palavras que façam parte de listas: evite palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc. Existem programas que tentam descobrir senhas combinando e testando estas palavras e que, portanto, não devem ser usadas.

### Dicas práticas que você pode usar na elaboração de boas senhas são:

-  Selecione caracteres de uma frase: baseie-se em uma frase e selecione a primeira, a segunda ou a última letra de cada palavra. Exemplo: com a frase "O Cravo brigou com a Rosa debaixo de uma sacada" você pode gerar a senha "?OCbcaRddus" (o sinal de interrogação foi colocado no início para acrescentar um símbolo à senha).
-  Utilize uma frase longa: escolha uma frase longa, que faça sentido para você, que seja fácil de ser memorizada e que, se possível, tenha diferentes tipos de caracteres. Evite citações comuns (como ditados populares) e frases que possam ser diretamente ligadas à você (como o refrão de sua música preferida). Exemplo: se quando criança você sonhava em ser astronauta, pode usar como senha "1 dia ainda verei os aneis de Saturno!!!".
-  Faça substituições de caracteres: invente um padrão de substituição baseado, por exemplo, na semelhança visual ("w" e "vv") ou de fonética ("ca" e "k") entre os caracteres. Crie o seu próprio padrão pois algumas trocas já são bastante óbvias. Exemplo: duplicando as letras "s" e "r", substituindo "o" por "0" (número zero) e usando a frase "Sol, astro-rei do Sistema Solar" você pode gerar a senha "SS0l, asstr0-rrei d0 SSistema SS0larr".