PERGUNTAS E RESPOSTAS - CONTRIBUIÇÕES

RES. 102/21 – CAPÍTULO III

Versão 1.0 – Junho de 2021

Índice

Este documento foi elaborado com base nas perguntas dirigidas a contribuicoes@fgc.org.br.

Regulatório: legislação, vigência e obrigações

1. Este Perguntas e Respostas ("FAQ") abrange também informações do Censo?

Resp.: - **NÃO**. Este Perguntas e Respostas concerne apenas às dúvidas mais comuns do Contribuições Res. BCB 102/21. Para as informações do Censo, consultar documento publicado em: https://fgc.org.br/associadas/censo

2. Qual a data que deveremos iniciar o envio da base de contribuição ao FGC, através do leiaute FGC405 – Base de Contribuição?

Resp.: - Uma vez que a Res. BCB 102/2021 entra em vigor em 1º (primeiro) de julho de 2021, a primeira remessa oficial em produção deverá ser encaminhada ao FGC até o dia 18 de agosto de 2021 referente ao fechamento de julho de 2021. **Lembramos que a Res. BCB 102/2021, que definiu essas datas.**

3. Até quando poderei enviar as informações por e-mail ao compesp conforme processo atual?

Resp.: - **Até o dia 15/07/2021, referente a base de contribuição de junho/2021**. Após esta data o processo por e-mail será desativado.

4. Posso enviar com valor zero as informações de Patrimônio Líquido Ajustado (PLA), Valor de Referência (VR) e Captações de Referência (CR)?

Resp.: - As instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil associadas ao FGC devem elaborar e remeter ao FGC, até o dia 18 (dezoito) de cada mês, as informações necessárias para o cálculo das contribuições ordinárias, especiais e adicionais devidas, referentes ao mês imediatamente anterior. Os valores das contribuições ordinárias e especiais devem ser calculados com base nos saldos, do último dia de cada mês, das contas e dos instrumentos financeiros representativos dos créditos objeto de garantia nos títulos e nos subtítulos do Plano

Contábil das Instituições do Sistema Financeiro Nacional (Cosif) divulgados pelo Banco Central do Brasil, os valores apurados são de responsabilidade da instituição financeira e devem ser encaminhados corretamente para o FGC.

5. Quando devo enviar ao FGC através da FGC405 – Base Contribuição as informações de contribuição?

Resp.: Deve ser enviado até o dia 18 do mês corrente, as informações referentes a base de contribuição conforme balancete do mês imediatamente anterior.

6. E se a IF ainda não possuir as informações de balancete do mês anterior para informar a base de contribuição o que eu faço?

Resp.: Até o dia 18 do mês corrente você poderá enviar a base de competência do mês anterior (mmCompetencia) utilizando a última informação de balancete de base de contribuição que tiver disponível (baseCompetencia). **Exemplo:** Durante o mês corrente de Junho/2021 até o dia 18, poderá enviar mmCompetencia (202105) a base devida é baseCompetencia (202105) ou na falta da conclusão do balancete deve utilizar baseCompetencia (202104), neste caso será necessário enviar uma retificadora de base de contribuição no mês subsequente.

7. Se eu enviei uma FGC405 informando mmCompetencia (imediatamente anterior ao mês corrente), com informação de balancete baseCompetencia de mês anterior e depois obtive a informação de balancete correta, posso corrigir?

Resp.: SIM, até o dia 18 sempre que você enviar uma FGC405 de Tipo de Base de Contribuição Inclusão (1) com mesmo mmCompetencia e tipoContribuicao já enviado anteriormente dentro do mês corrente, a informação enviada anteriormente será cancelada, passando a valer a informação mais recente enviada através da FGC405.

8. E se eu não enviar as informações até o dia 18, posso enviar do dia 19 em diante?

Resp.: NÃO, o sistema será fechado para envios da FGC405 a partir de 0(zero) hora do dia 19 até o final do mês, reabrindo no próximo dia 01 para envio das informações da competência seguinte e de retificadora do mês em que não cumpriu a obrigação até a data limite.

9. O que o FGC fará quando eu não entregar a base de contribuição através da FGC405 até o dia 18?

Resp.: O FGC irá calcular o valor da contribuição com base na última base de contribuição

entregue e enviará as informações calculadas e o número de controle para consulta por e-mail para os endereços cadastrados como Contato Contábil e para os e-mails enviados na FGC405 anterior. Ressaltamos que o pagamento deverá ser realizado pelo fluxo normal do STR da mesma forma que a contribuição enviada. O modelo do e-mail a ser enviado pelo sistema do FGC está detalhado abaixo:

Remetente: noreply@fgc.org.br

Assunto: [FGC - Contribuições] – NAO ENVIO DE BASE DE CALCULO DA CONTRIBUICAO ATE A DATA LIMITE 18/MM/AAAA

Corpo do E-mail:

Prezados Senhores,

Devido ausência de informação até as 23h59 de ontem, data limite para envio das informações referentes a base de contribuição, PLA, VR e CR para a competência de MM/AAAA foi aplicado o parágrafo Art.10 da Resolução 102/21, para apuração dos valores de contribuição cujo recolhimento deverá ocorrer até o primeiro dia útil do próximo mês.

Segue valores:

Competência: AAAAMM

Base de Competência: AAAAMM04

Valor da Base da Contribuição: R$ 000.000.000,00 Valor do Patrimônio Líquido Ajustado: R$ 00.000.000,00 Valor de Referência: R$0000000,00 Valor Capitação de Referência Anterior: R$ 00.000.000,00 ID Contribuição: 12345678020620210000000209028 O valor da Contribuição devida poderá ser consultado utilizando o Número de Controle: 02062021000000339879931234567 8.

Informamos que entre os dias 1 e 18 do próximo mês, está instituição financeira deverá providenciar o envio de informação retificadora dos valores corretos da data base MM/AAAA

Atenciosamente,

FGC

10. Se eu enviei no mês anterior uma FGC405 de inclusão (Tipo de Base de Contribuição =1) com informação de baseContribuicao de meses anteriores como faço para corrigir a informação enviada nesse mês atual?

Resp.: Deverá ser enviada uma FGC405 com Tipo de Base de Contribuição Retificadora (2), informando o mmCompetencia e a baseCompetencia que está sendo corrigida. Sempre neste envio de retificadora as informações de mmCompetencia e baseCompetencia devem ser iguais.

11. Existe a possibilidade do mmCompetencia e baseCompetencia serem diferentes?

Resp.: Sim, somente para o Tipo de Base de Contribuição =1 (inclusão), quando até o prazo regular da entrega da contribuição (dia 18 de cada mês) a Instituição não possuir os valores de balancete do mês imediatamente anterior para informar, pode ser enviada uma contribuição de inclusão (tipoBaseContribuicao = 1), cujo mmCompetencia será o mês imediatamente anterior (ou seja, o mês regular a entrega da contribuição) e o baseCompetencia seguirá a informação do valor do balancete informado, ou seja, mês -2. **Exemplo:** durante o mês de corrente de julho entre os dias 01 e 18 de julho deve ser entregue a contribuição de inclusão:

mmCompetencia: 202106

baseCompetencia: 202106

tipoBaseContribuicao: 1

Porém, caso os valores do balancete de junho, não estejam disponíveis a Instituição poderá enviar a inclusão dessa forma, para cumprir o prazo regular:

mmCompetencia: 202106

baseCompetencia: 202105

tipoBaseContribuicao: 1

Sempre que uma inclusão for efetuada com valor de balancete diferente da competência da contribuição, obrigatoriamente a Instituição deve enviar uma retificadora do mês seguinte além da contribuição de inclusão do mês, exemplo de como seria a retificadora que neste exemplo deverá sem entregue entre os dias 01 e 18 de agosto:

mmCompetencia: 202106

baseCompetencia: 202106

tipoBaseContribuicao: 2

12. Se eu não efetivar o pagamento do valor da(s) Contribuição(ões) até o primeiro dia útil e for necessário o pagamento de Multa como será o procedimento?

Resp.: O pagamento do principal e da Multa deverão ocorrer através de STR distintas com as respectivas finalidades, ou seja, os valores não podem ser somados. O FGC irá calcular conforme Art. 12º da Res. BCB 102/21 e informar através de e-mail os valores para recolhimento, conforme exemplo abaixo, os valores também poderão ser consultados através da FGC406, utilizando o número de controle informado:

Remetente: noreply@fgc.org.br

Assunto: [FGC - Contribuições] – ATRASO NO RECOLHIMENTO DA CONTRIBUIÇÃO E RESPECTIVA MULTA.

Corpo do E-mail:

Prezado(a),

MULTA:

Conforme Art. 12º da Res. BCB 102/21 "O atraso no recolhimento das contribuições devidas sujeita a instituição associada ao FGC responsável pela contribuição a multa de 2% (dois por cento) sobre o valor da contribuição, acrescido de atualização com base na taxa Selic.

Segue informação de valor dos encargos devidos:

Competência: AAAAMM

Base de Competência: AAAAMM

Valor da Multa: R$ 0.000,00 o recolhimento da multa deverá ser feito através de STR004 finalidade 145

ID Contribuição Multa: 12345678316042021152318254361202103

O valor da Contribuição devida e da Multa poderá ser consultado utilizando o Número de Controle: 12345687182318339877937066413 4.

Atenciosamente,

Fundo garantidor de créditos.

Layout dos arquivos

13. Porque logo após o envio da FGC405 eu consulto os valores através da FGC406 e os valores retornam nulos (null)?

Resp.: O FGC406R somente irá retornar informações com valores calculados, após o FGC realizar o cálculo e enviar para a Credenciada este processo acontece entre os dias 19 – 25 de cada mês, ou seja, a garantia de retorno com valores no FGC406R é somente a partir do dia 26, porém poderá ser disponibilizado antes, mas sempre após o dia 19. Os valores calculados também devem ser consultados através da FGD001 na Instituição Financeira Credenciada conforme manual disponível em nosso site https://fgc.org.br/associadas/contribuicoes

14. Quando vou receber cada um dos Status de Contribuição no retorno da FGC406?

Resp.: Até o dia 18 de cada mês é a janela para envio das bases de contribuição, sempre que entregue com sucesso até o dia 18 ao consultar o FGC406 receberão um retorno com valores null e o statusContribuicao = 1 (A calcular).

No dia 19 é efetuado o cálculo da contribuição e o statusContribuicao passa a ser 2 (calculado), porém ainda neste momento o retorno da FGC406 será null.

Entre os dias 19 e 25 de cada mês após validação dos valores calculados o FGC irá direcionar os valores a IF Credenciada, neste momento o statusContribuicao passa a ser 3 (Disponível) e o FGC406R passa a retornar valores. Lembrando isso pode acontecer a qualquer momento dentro desse intervalo de dias, ou seja, a garantia de retorno com valores no FGC406R é somente após o dia 26, porém pode ser que seja disponibilizado antes, mas sempre após o dia 19.

O vencimento da contribuição devida é sempre até o primeiro dia útil do mês subsequente, então quando o FGC receber a confirmação de pagamento da IF Credenciada o statusContribuicao será atualizado para 5 (Recolhido), neste momento a FGC406R retornara com valores e statusContribuicao = 5.

Em caso de não pagamento da contribuição na data, o statusContribuicao a partir do segundo dia útil será 4 (Em Aberto), e a FGC406R irá retornar com valores e statusContribuicao = 4.

Se dentro do período de 01 a 18 de cada mês, e for enviado por mais de uma vez a mensagem FGC405 com o mesmo mmCompetencia para o mesmo tipoContribuicao e tipoBaseContribuicao já enviado anteriormente dentro desse mesmo período, alteramos O ENVIO ANTERIOR para o statusContribuicao = 9 (Cancelado) e consideramos o envio mais atual como válido.

API e comunicação

15. De que forma eu devo enviar as informações do Contribuições para o FGC?

Resp.: - As Instituições Financeiras (IFs) devem desenvolver seus próprios sistemas para transmissão das informações de Contribuição ao FGC, ou então comprar uma solução de mercado que faça esse trabalho.

Existem soluções prontas de mercado que a IF pode adquirir, mas o FGC não pode indicar ou dar preferência a nenhuma dessas soluções, nem garantir que funcionem.

É responsabilidade da IF testar as aplicações para garantir que conseguem se comunicar com o FGC.

16. Eu posso transmitir as informações do Contribuições por outro meio (site na internet, e-mail, FTP, pendrive entregue em mãos, documento impresso etc)?

Resp.: - NÃO. A Instituição Financeira deve **obrigatoriamente** desenvolver um sistema para envio dessas obrigações ao FGC, ou adquirir no mercado uma solução pronta que faça isso. O FGC não irá, em hipótese alguma, indicar ou dar preferência a nenhuma dessas soluções, nem garantir que funcionem.

É **responsabilidade exclusiva da IF** testar as aplicações, sejam de mercado, sejam desenvolvidas internamente, para garantir que conseguem se comunicar com o FGC. O FGC prestará todo o suporte necessário para a execução desses testes.

17. Como esse sistema de transmissão do Contribuições deve funcionar?

Resp.: - As informações a seguir são destinadas ao pessoal de TI e aos desenvolvedores da aplicação. Caso você não entenda o que está sendo descrito, solicite ajuda ao seu departamento de TI.

A comunicação entre a Instituição Financeira (IF) e o FGC se dará por uma API nossa, disponível publicamente na Internet. Essa API receberá os dados de Contribuições, conforme o Manual Técnico, disponibiliza webservices em arquitetura REST. As transmissões serão enviadas em arquivos de dados no formato JSON.

A conexão à API, em nível de rede, se dá por HTTPS via porta TCP/443 – ou seja, é uma conexão Web com TLS/SSL, mas **não** serão transmitidos arquivos HTML. Em vez disso, serão transmitidos dados em formato JSON.

As informações serão transmitidas por meio de um túnel criptografado TLS/SSL para garantir sigilo e segurança (mais detalhes no Manual e neste Perguntas e Respostas).

18. Eu posso testar a API para validar meu sistema de envio do Contribuição?

Resp.: - SIM. A homologação é obrigatória! Você precisará homologar sua aplicação no FGC antes de começar as entregas definitivas. Mais informações sobre homologação podem ser obtidas no Plano Homologatório.

19. A homologação é obrigatória?

Resp.: - SIM! A homologação é obrigatória pois serve a dois propósitos muito importantes, que devem ser levados em conta no desenvolvimento da aplicação:

1. Experimentar e validar a aplicação durante seu desenvolvimento;
2. Validar as informações a serem enviadas futuramente ao Contribuições de produção.

Mais informações sobre homologação podem ser obtidas no Plano Homologatório.

20. O que eu preciso homologar?

Resp.: - Aquilo o que está descrito no Plano Homologatório. Lembre-se de que você está homologando duas coisas: a aplicação que está sendo desenvolvida para envio do Contribuições ***e*** a Instituição Financeira, portanto é necessário realizar os testes com a própria aplicação definitiva. Em resumo:

- **Desenvolvedor:** deve validar **todos os itens do Plano Homologatório**, para ter certeza de que todas as mensagens e campos estão consistentes. O desenvolvedor pode usar softwares de teste de APIs (como por exemplo Postman e Advanced Rest

Client - ARC, citados no Manual) para testes preliminares e ensaios, mas para homologar deve usar a própria aplicação que está desenvolvendo.

- **Instituição Financeira (IF):** deve validar apenas os itens citados como obrigatório do Plano Homologatório. A IF deve homologar-se para: 1. Comprovar que o software instalado na IF está de acordo com a tecnologia do Contribuições, 2. Validar se os colaboradores da IF sabem operar o software e 3. Validar que os dados estão vindo da origem correta e não de impostores. Essa homologação **não deve** ser feita com software de testes (i.e., não deve usar Postman e ARC) mas sim ser realizada com a própria aplicação adquirida pela IF. Os testes devem ser feitos com dois tipos de valores: payload zerado, e payload com valores consistentes em todos os campos.

Mais informações sobre homologação podem ser obtidas no Plano Homologatório.

21. Após envio do cadastro técnico e chave pública, o FGC enviou um e-mail dizendo que poderíamos testar os ambientes de homologação e produção. No manual sugerem instalar ferramentas como Postman e ARC. Poderiam me explicar o que especificamente devemos fazer? Nosso time de IT deve instalar essas APIs (sic) e depois testar com os logins?

Resp.: - "Testar o ambiente" significa fazer todos os testes e validações descritos no Plano Homologatório. Seguir o plano homologatório à risca é obrigatório para que o sistema de produção seja liberado. Quem não realizar as validações descritas no Plano Homologatório estará impedido de entregar as obrigações do Contribuições em produção.

As ferramentas Postman e ARC devem ser usadas pelo **desenvolvedor da aplicação** adquirida pela Instituição Financeira (IF) para testar a API do FGC. Os testes devem servir como base para o desenvolvimento do sistema na IF. O pessoal operacional/financeiro da IF não deve usar essas ferramentas.

Por fim, as APIs são as URLs (ou seja, endereços na Internet) descritas no Plano Homologatório. Elas não são "instaladas" na Instituição Financeira (IF). O que é instalado na IF é um sistema de envio dos arquivos do Contribuições. Esse sistema é que se conecta à API (ou seja, acessa as URLs) do FGC.

22. Como eu descubro o endereço da API para poder me conectar?

Resp.: - As URLs das APIs na Internet estão declaradas no Plano Homologatório.

23. Eu cliquei com o mouse diretamente no link da API (indicada no Plano Homologatório) e recebi uma mensagem de erro **405 Method Not Allowed**. Por que não deu certo?

Resp.: - As APIs não foram feitas para se clicar diretamente com o mouse, ou acessadas pelo navegador. Quando se tenta abrir o link da API com um navegador comum – Edge, Firefox, Chrome, Safari ou qualquer outro – aparece essa mensagem de erro, **que está correta**.

Para testar as APIs, utilize os **aplicativos de teste** mencionados no **Manual Operacional e Técnico – CENSO**, seção **7.1 API Rest (JSON)**, página 12 (Postman e ARC - Advanced Rest Client). Também é possível testar as APIs diretamente no Portal do Desenvolvedor do FGC, a ser divulgado em breve (este FAQ será atualizado para indicar a URL do futuro Portal do Desenvolvedor).

Entretanto, **recomendamos que apenas desenvolvedores e pessoal de TI façam testes com a API**. Se você não for desenvolvedor ou TI, aguarde a implementação do sistema definitivo, **que deve ser desenvolvido pela Instituição Financeira ou comprado no mercado**.

24. O FGC presta suporte às aplicações Postman e ARC – Advanced Rest Client?

Resp.: - NÃO. Procure suporte junto ao desenvolvedor de cada aplicação. Voltamos a ressaltar que essas são aplicações de teste para desenvolvedores e equipe de TI, e não devem ser usadas pela equipe operacional/financeira da Instituição Financeira.

25. O FGC presta suporte às aplicações de mercado adquiridas pela Instituição Financeira (IF) para transmitir os dados do Contribuições?

Resp.: - NÃO. Procure suporte junto ao fornecedor que vendeu a solução para a Instituição Financeira.

26. Caso eu desenvolva internamente minha própria aplicação para transmitir os dados do Contribuições, terei suporte técnico do FGC?

Resp.: - SIM, mas **apenas** para os seguintes pontos:

- Dúvidas sobre os leiautes dos arquivos
- Dúvidas sobre o Swagger
- Dúvidas sobre a API
- Dúvidas sobre Conexão e Certificado Digital

27. Existe alguma documentação da API como um endereço "api-doc", por exemplo?

Resp.: - NÃO. Não existe documentação on-line das APIs. Os endereços de comunicação via API constam nos manuais técnicos disponíveis no site do FGC. Toda a informação necessária está nesses manuais. Casos omissos devem ser dirimidos pelo e-mail contribuicoes@fgc.org.br.

28. Qual o CHARSET a ser utilizado para transmissão das mensagens JSON? (UTF8 ou UTF16)

Resp.: - Deverá sempre ser utilizado UTF-8.

29. "Todos os dados trafegados no ambiente de **homologação** deverão ser descaracterizados". A palavra "**descaracterizados"** indica que as informações devem ser criptografadas?

Resp.: - NÃO. Não é necessário criptografar nada no ambiente de homologação. O que deve ser feito é a descaracterização dos dados sensíveis. Para descaracterizar basta substituir os dados pessoais ou sensíveis por dados aleatórios. **A descaracterização é obrigatória para aderência à LGPD e é de responsabilidade exclusiva da Instituição Financeira.** O FGC não fará nenhuma verificação nem será responsável por vazamento de dados pessoais em caso de falha da IF em descaracterizar seus dados de homologação.

30. Todos os novos documentos e informações devem ser transmitidos por meio do certificado?

Resp.: **NÃO**. Apenas os arquivos em formato JSON enviados pela API. O certificado é usado em dois momentos:

- Para garantir a autenticação por ***Mutual TLS Authentication*** antes de estabelecer a conexão segura com a API.
- Após o estabelecimento da conexão, o certificado completo da IF é novamente enviado no cabeçalho (*header*) de cada arquivo JSON transmitido, no campo "X-client-certificate", para validação de cada mensagem.

O cadastro técnico e Certificado contendo a chave pública devem ser encaminhados via e-mail apontado no manual técnico que consta no Site do FGC (contribuicoes@fgc.org.br).

31. Com relação à chave de acesso [fornecida pelo FGC para a Instituição Financeira], teremos que mandar o Certificado Digital para o FGC toda vez que o renovarmos, ou a chave de acesso fornecida pelo FGC é única e vale indefinidamente?

Resp.: - SIM, é necessário reenviar o certificado e aguardar nova chave de autenticação. Todo Certificado Digital tem um prazo de validade ("expira em") e a chave de acesso gerada pelo FGC considera essa data de vencimento. Todas as vezes que o certificado for renovado, a Instituição Financeira associada tem a obrigação de o reenviar para que o FGC possa gerar a nova chave de acesso.

Lembramos que os Certificados Digitais a serem usados no Contribuições devem ter validade de um (01) ano – ou seja, devem ser renovados todos os anos. É responsabilidade da Instituição Financeira controlar o vencimento de seu

próprio Certificado.

32. O manual cita que a comunicação "exige certificado digital na chamada". Deve ser enviado no header a chave "x- client-certificate" contendo o mesmo certificado enviado previamente ao FGC junto ao cadastro técnico. Esse certificado que é citado no texto se refere à chave pública que foi enviada junto ao cadastro técnico ou o próprio certificado em si?

Resp.: - Existe uma confusão de termos entre **Certificado Digital**, **Chave Pública** e **Chave Privada**. Mais adiante neste documento, incluímos uma explicação mais detalhada sobre o que é cada um desses itens.

Respondendo à pergunta, a API-Key "x-client-certificate" refere-se ao arquivo .TXT ou .CER do Certificado Digital adquirido pela Instituição Financeira e encaminhado ao FGC. Dentro do Certificado está a Chave Pública, mas é para enviar o Certificado completo, sem a chave privada. O certificado deve ser no padrão X.509, em formato texto (PEM), codificado em ASCII Base64 conforme o Manual Técnico e Operacional.

Obs.: **NÃO** deve ser encaminhado ao FGC o arquivo .KEY contendo a chave privada, nem certificados tipo Keychain nos formatos .JKS, .PFX ou .P12 (Certificados em formato binário que já possuem a chave privada embutida). **Somente** o Certificado Digital contendo apenas a Chave Pública, em formato texto (PEM), é que deve ser enviado ao FGC.

Para mais informações, consulte a seção *Certificado Digital, Chave Pública e Chave Privada* nas próximas páginas.

33. Então vou usar o meu Certificado Digital duas vezes para cada transmissão de arquivo, uma vez na autenticação SSL e a outra dentro da mensagem JSON?

Resp.: - SIM. É exatamente esse o mecanismo.

34. Todas as mensagens serão assinadas pela Chave Privada do remetente. Como deve ser realizada a assinatura?

Resp.: - Não há necessidade de assinatura. Apenas devem ser enviados os dados obrigatórios no cabeçalho (*header*) da mensagem conforme Swagger, Manual e Plano Homologatório. Devido à segurança da autenticação prévia por ***Mutual TLS Authentication***, não é necessário assinar digitalmente cada mensagem.

Consultar a próxima pergunta para mais informações.

35. Todo tráfego de informações deverá ser criptografado pelas Instituições Financeiras. Como

devem ser realizados os passos de criptografia? Será necessária alguma etapa adicional ou a própria utilização do certificado digital já garante a segurança do tráfego?

Resp.: - A segurança do tráfego de dados entre as Instituições Financeiras e o FGC é realizada em duas camadas: **conexão segura** (HTTPS) e **autenticação em dois níveis**.

- **Conexão segura**: a aplicação da Instituição Financeira e o sistema do Contribuições no FGC estabelecem, no início da transação, um canal seguro de comunicação. Esse canal é criptografado usando o protocolo HTTPS (HTTP com SSL/TLS).
- **Autenticação em dois níveis**:
  - **Primeiro nível de autenticação**: implementado pela própria conexão HTTPS, pois é realizada uma verificação de identidade chamada ***Mutual TLS Authentication***, na qual o FGC verifica a idoneidade do Certificado Digital da Instituição Financeira, e a Instituição a idoneidade do Certificado do FGC.
  - **Segundo nível de autenticação**: é implementado nas próprias mensagens enviadas, pois **a API só aceita mensagens que tragam, no *header*, três chaves de autenticação de API (API-Keys):**
    - **As duas chaves encaminhadas pelo FGC** (**X-Client-ID** e **X-Client-Secret**), disponibilizadas apenas após o envio, pela IF, do Cadastro Técnico e do Certificado Digital da Instituição ("chave pública");
    - **O próprio Certificado Digital da IF**, que é embutido dentro das mensagens enviadas (chave X-Client-Certificate).

36. O ambiente de homologação estará sempre disponível para testes? Caso esteja, podemos manter o uso do certificado "auto assinado"?

Resp.: - SIM. O ambiente de homologação estará sempre disponível.

Observe apenas que o certificado auto assinado da homologação também deve ter prazo de validade de um ano e que, **30 dias antes de expirar**, o certificado deve ser renovado e enviado ao FGC. Serão geradas novas chaves de acesso, que devem ser cadastradas no sistema da instituição. **Isso ocorrerá anualmente e vale tanto para o ambiente de homologação quanto o de produção, então pedimos atenção à validade dos certificados para não interromper a comunicação. É responsabilidade da Instituição Financeira controlar a validade de seus próprios Certificados Digitais.**

Certificado Digital, Chave Pública e Chave Privada

INFORMAÇÕES GERAIS SOBRE CERTIFICADOS DIGITAIS

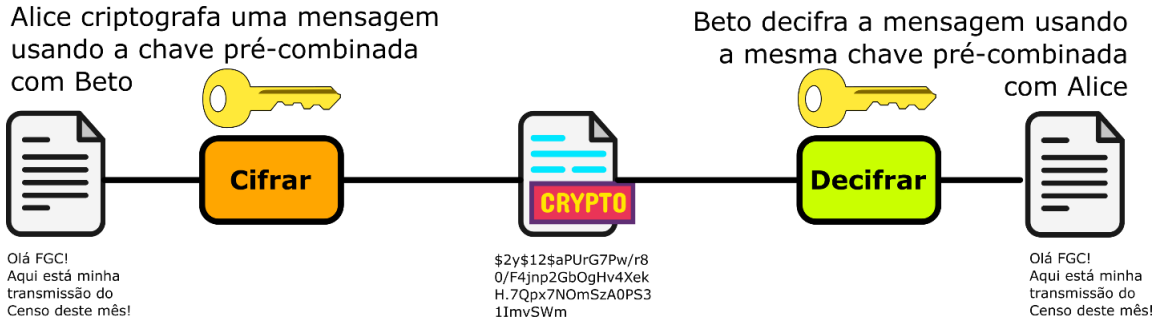
37. O que é criptografia?

Resp.: - Criptografia é uma técnica que permite proteger dados, tanto dados em trânsito (sendo movimentados em uma rede, ou na internet) como dados em repouso (guardados, por exemplo, num *pendrive*). A criptografia codifica os dados para que eles fiquem irreconhecíveis e ilegíveis.

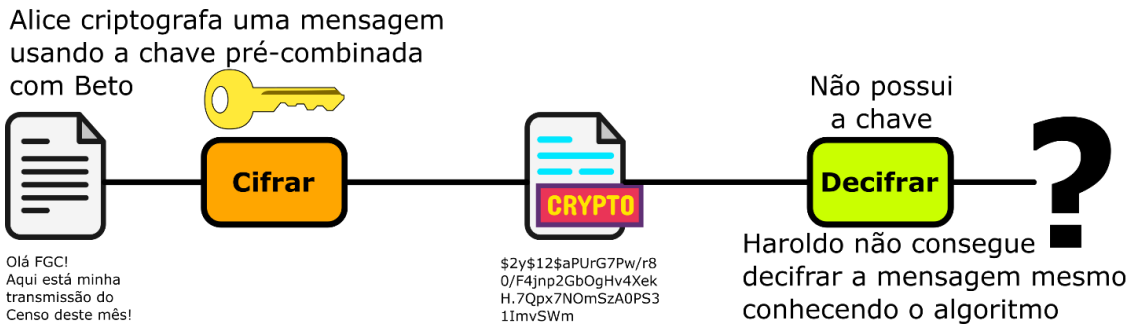
Para cifrar (ou seja, criptografar) e decifrar os dados, são necessárias duas coisas:

- Um método de criptografia, chamado de **algoritmo**. Esse método é usado como "receita" para cifrar e decifrar as mensagens.
- Uma senha, chamada de **chave**.

Tanto para cifrar quanto para decifrar (ou seja, "descriptografar") os dados, é necessário usar uma chave. Apenas quem tem a posse dessa chave consegue ler os dados criptografados.



Mesmo que alguém saiba o algoritmo usado para criptografar uma mensagem, se essa pessoa não tiver a chave usada no momento da cifragem, não conseguirá decifrar.



Quando se usa a mesma chave para criptografar e descriptografar, chamamos esse algoritmo de **criptografia com chave simétrica**. É por isso que esse tipo de criptografia também é chamado de **Segredo Compartilhado (*Shared Secret* ou *Shared Key*)**.

38. O que é Chave Pública? O que é Chave Privada?

Resp.: - O algoritmo de chave simétrica (consulte a resposta anterior) tem um problema de segurança: é preciso que o remetente e o destinatário compartilhem a mesma chave. Todo segredo em algum momento é revelado, então não é uma estratégia muito segura.

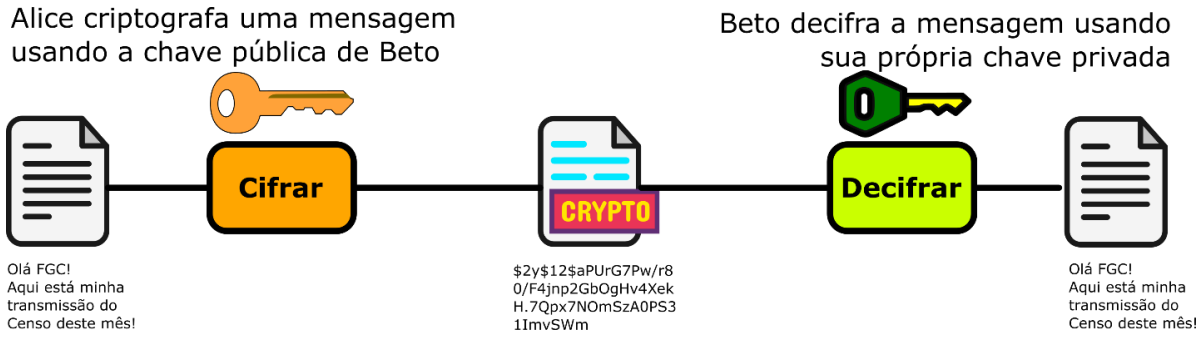
Para tornar o sistema bem mais seguro, criou-se um outro tipo de criptografia, com duas chaves. Uma chave é usada para criptografar os dados. A outra chave é usada para descriptografar. Por usar duas chaves diferentes, esse algoritmo é chamado de **criptografia de chave assimétrica**.

Uma das chaves é chamada de **Chave Privada**, e apenas o dono da chave tem acesso a ela. É um segredo, não pode revelar para ninguém, nem para o companheiro de comunicação. A Chave Pública deve ser guardada por seu dono da forma mais segura possível. É um dos ativos de maior valor dentro de uma infraestrutura de TI.

A outra chave é chamada de **Chave Pública**, e pode ser distribuída livremente para o mundo inteiro. O que é criptografado pela chave pública só pode ser descriptografado pela chave privada, e vice-versa.

Aproveitando o exemplo da pergunta anterior, para Alice criptografar uma mensagem destinada a Beto, Alice usa a chave pública de Beto. Esse detalhe é importante: Alice vai mandar uma mensagem a Beto, então Alice usa a chave pública do Beto, não a dela mesma!

Qualquer um pode criptografar mensagens usando a chave pública de Beto, mas **apenas Beto conseguirá lê-las** com sua chave privada (que ele guarda num cofre bem protegido e não revela a ninguém).



39. O que é Certificado Digital?

Resp.: - Usando criptografia assimétrica, podemos ter certeza de que apenas o

destinatário irá ler os dados transmitidos (veja a pergunta anterior). Entretanto, como ter certeza de que a chave pública que usamos para cifrar a mensagem era mesmo do destinatário? Podemos usar a chave pública de um impostor sem saber.

Para garantir que a chave pública pertence realmente ao destinatário, essa chave pública tem sua autenticidade garantida por um **Certificado Digital**. Esse Certificado é emitido por uma entidade que funciona como um "cartório digital". Esse "cartório", chamado de Autoridade Certificadora (ou, simplesmente, AC) garante que o Certificado (e, portanto, que a Chave Pública que está dentro dele) pertence realmente a seu dono.

O Certificado Digital é um arquivo. Dentro desse arquivo estão:

- A Chave Pública
- Informações sobre o dono do Certificado (também dono da Chave Pública)
- Informações sobre a Autoridade Certificadora (AC) para que a autenticidade do Certificado possa ser verificada.

40. Por que eu preciso de um Certificado Digital?

Resp.: - Um certificado Digital é necessário quando:

- Preciso me identificar para outras pessoas ou instituições, e para isso mostro meu Certificado Digital. Essas pessoas ou instituições irão consultar a CA que emitiu o Certificado para me "autenticar", ou seja, verificar se eu sou quem digo ser.
- Preciso que as pessoas acessando meu website ou sistema na internet tenham certeza de que estão acessando o ambiente legítimo e não um sistema impostor.
- Preciso criar um canal criptografado pelo qual trafegarei informações com segurança. Esse canal em algum momento usará minhas chaves pública e privada.

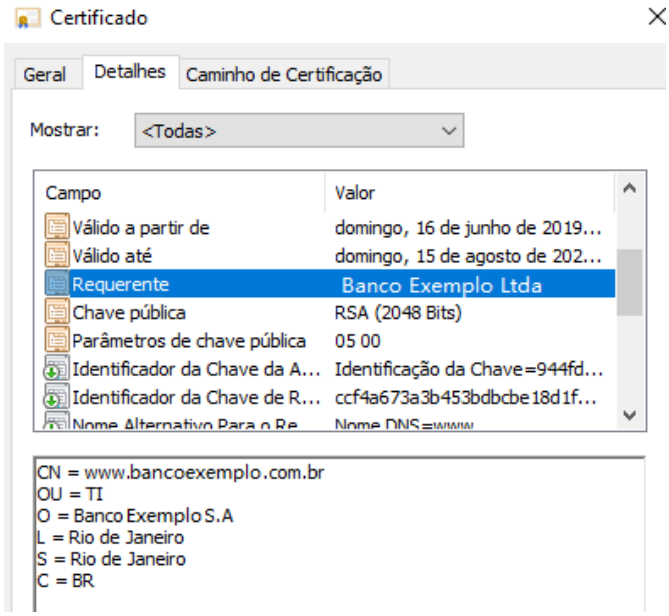
41. O que é PKI, *Public Key Infrastructure*?

Resp.: - PKI, (*Public Key Infrastructure*, em português Infraestrutura de Chave Pública) é um arranjo de sistemas, processos, normas e entidades que garantem a validade e a idoneidade de Certificados Digitais na Internet. O PKI funciona pelo método do Endosso: quando alguém adquire um Certificado Digital, alguma entidade reconhecida mundialmente o assina digitalmente, garantindo que o certificado adquirido é válido.

42. Como posso consultar as informações dentro do meu Certificado Digital?

Resp.: - No Windows, é possível abrir um certificado digital clicando duas vezes no arquivo do Certificado.

Para que o Windows possa acessar as informações (campos), o nome do arquivo que contém o certificado deve ter a extensão .CER. Caso o arquivo tenha a extensão .TXT, renomeie-o para .CER. Dessa forma, ao clicar duas vezes no arquivo, o Certificado será aberto no Gerenciador de Certificados do Windows e não no Bloco de Notas.



Ao abrir, aparecerá uma janela, e nela podemos navegar nas diferentes informações que estão gravadas em seu interior.

Clique na aba **Detalhes**, e depois clique em cada um dos campos para exibir seus dados.

43. Que informações existem dentro de um Certificado Digital? O que são os campos do Certificado Digital?

Resp.: - Dentro do Certificado Digiyal, algumas informações são de interesse apenas do sistema, outras existem para identificar precisamente o dono do certificado. Cada informação existente no certificado está guardada em um **Campo**, e dentro do campo podemos ter um ou mais **Identificadores**. Na imagem da pergunta anterior, vemos selecionado o campo Requerente, e no painel inferior, todos os identificadores associados ao campo Requerente.

Dentre os **campos** de maior interesse, podemos destacar:

- **Chave Pública**: sequência realmente grande de caracteres atribuídos a um campo dentro do Certificado.
- **Emissor**: Entidade que emitiu o Certificado (normalmente uma Autoridade Certificadora – AC).
- **Requerente**: entidade que solicitou (ou seja, comprou) o Certificado Digital.
- **Validade**: datas de início de validade e expiração do certificado.

Dentro dos campos, pode haver um ou mais identificadores. Por exemplo, no **campo Requerente** (em inglês, *Subject*) é possível ter os seguintes identificadores:

- **Organização (O)**: nome da empresa ou entidade que solicitou o certificado.
- **Divisão/Departamento (OU)**: departamento, divisão, setor ou área da empresa responsável pelo certificado. Pode haver várias OUs no certificado, e as OUs podem ser utilizadas para armazenar qualquer dado (por exemplo, o CNPJ do requerente). A sigla OU indica *Organizational Unit* (unidade organizacional).
- **Localidade (L)**: Cidade ou qualquer outro indicador de localidade.
- **Estado (S)**: Estado, província ou qualquer outra unidade de organização do país. S é do inglês State.
- **País (C)**: sigla ISO de duas letras indicando o país. (C = Country). Para o Brasil, a sigla ISO é **BR**.

OBS: esta é a descrição de um Certificado Digital genérico. Para o Certificado Digital específico do FGC, consulte as próximas páginas.

44. Obtendo um Certificado Digital

Resp.: - Para obter um Certificado Digital, é necessário entrar em contato com uma Autoridade Registradora (AR) e comprar o Certificado comercializado por eles. Há inúmeros tipos de Certificados, é necessário comprar o Certificado adequado a cada caso. Para conhecer as ACs e ARs existentes, consulte **https://estrutura.iti.gov.br/**

Será necessário gerar e entregar à AR um arquivo chamado CSR (*Certificate Signing Request*), e a partir desse arquivo a Autoridade Certificadora (AC) associada à AR irá gerar um Certificado Digital assinado (ou seja, garantido) por ela.

Consulte a AR que fornecerá o Certificado Digital para mais informações sobre como gerar o CSR. Mais informações sobre CSR nas próximas perguntas.

45. Estou confuso. O que é uma AR e o que é uma AC? Por que eu comprei o Certificado de uma empresa mas foi emitido por outra?

Resp.: - Em termos simples, a Autoridade Certificadora (AC) é quem emite e endossa o Certificado Digital. A AR (Autoridade Registradora), de forma simplificada, age como uma "revenda" da AC. Por isso, embora o certificado seja adquirido através da AR, a assinatura no campo Emissor do Certificado será a da AC.

46. O que é CSR (Certificate Signing Request)?

Resp.: - CSR (*Certificate Signing Request*) é um arquivo entregue à Autoridade Registradora (AR) para em troca obter um Certificado Digital.

O CSR é um bloco de texto, codificado de uma certa maneira, em formato de arquivo. Normalmente (mas nem sempre) o CSR é gerado no próprio computador onde o Certificado Digital será instalado.

Esse CSR será repassado pela AR a uma Autoridade Certificadora (AC), que emitirá o Certificado Digital a partir do CSR e dará a garantia de que é válido e legítimo – ou seja, será assinado pela AC.

O CSR deve indicar claramente quem é seu proprietário no campo **Requerente** – a saber, a pessoa ou entidade que solicitou o Certificado.

47. Que informações existem dentro de um CSR?

Resp.: - O CSR e o Certificado Digital têm praticamente as mesmas informações gravadas dentro deles - afinal, o CSR é usado para gerar o Certificado. Por exemplo:

- Nome da organização
- Cidade
- Estado
- País
- Chave Pública.

Diferente do Certificado Digital, o CSR não possui as informações do Emissor – estas serão preenchidas pela AC que emitirá o Certificado.

48. O que eu faço com a Chave Privada que é gerada junto com o CSR?

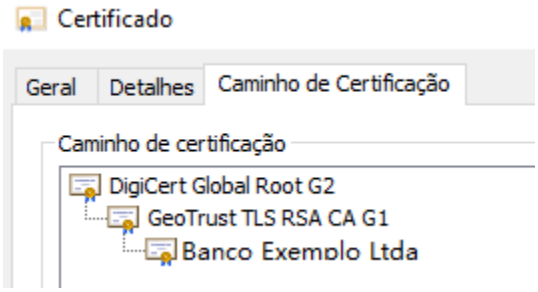
Resp.: - A chave privada normalmente é gerada ao mesmo tempo que o CSR, mas é um arquivo separado (normalmente de extensão .KEY). A Autoridade Certificadora (AC) irá usar o CSR para criar o Certificado Digital, mas nem a AR nem a AC podem receber ou ter conhecimento da Chave Privada. **Nunca envie o arquivo .KEY para a AR, nem para a AC, nem para o FGC!**

A Chave Privada deve ser instalada, junto com o Certificado Digital, no computador que vai usá-la, dentro da Instituição Financeira. O Certificado Digital instalado no Servidor só funciona em conjunto com a Chave Privada, portanto se a chave privada for perdida, o Certificado não funcionará.

A Chave Privada não deve ser distribuída nem revelada a ninguém!

49. O que é Caminho de Certificação?

Resp.: - O Certificado Digital precisa ser endossado (ou seja, assinado), por uma Autoridade Certificadora. Essa AC pode por sua vez ser endossada por uma AC de nível mais alto, e assim sucessivamente até chegar na AC de topo, também conhecidas como AC Raiz (em ingês, *Root Certification Authority* ou, simplesmente, *Root CA*).



Existem poucas e facilmente reconhecíveis ACs Raiz no mundo, e as ACs de nível mais baixo funcionam mais ou menos como "distribuidoras" dessa AC Raiz. A hierarquia entre todas as ACs do certificado é mostrada no Caminho de Certificação. Para verificar o Caminho de Certificação de um certificado, estando no Windows, clique duas vezes no Certificado para abri-lo, depois clique na aba **Caminho de Certificação**. Observe que a AR (Autoridade Registradora), que funciona como uma espécie de "revenda" das ACs, não aparece no Caminho de Certificação.

50. O que é um Certificado Digital auto assinado?

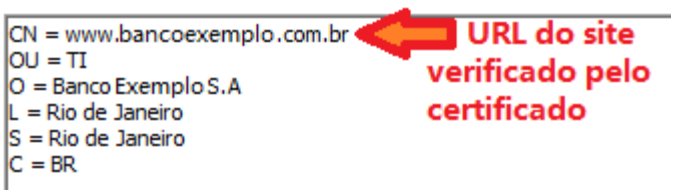
Resp.: - É um Certificado Digital gerado pela própria pessoa ou empresa.

Em termos de criptografia e conexão segura, ele funciona da mesma forma como um Certificado Digital emitido por uma Autoridade Certificadora (AC). A única diferença é na autenticação (verificação de identidade): um Certificado Digital auto assinado **não** é endossado por uma AC, portanto **não** há maneira de verificar a sua origem e titularidade.

Basicamente, um certificado auto assinado é um CSR assinado apenas com a própria Chave Privada. **Para os sistemas Censo e Contribuições, os certificados auto assinados só poderão ser utilizados em ambiente de homologação**.

51. Como funciona o Certificado Digital como validador de domínio?

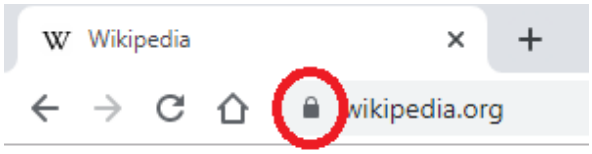
Resp.: - O Certificado Digital tem várias informações gravadas dentro dele. Uma dessas informações pode ser a URL (por exemplo, www.facebook.com) ou o domínio (por exemplo, todas as URLs que terminam em facebook.com). Quando o certificado



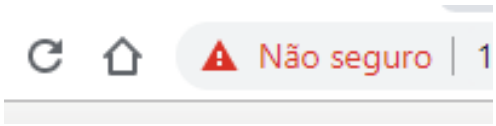
possui essa informação, pode ser usado para validar a identidade de websites e sistemas.

A URL do domínio ou site deve estar em um identificador **Common Name (CN)**, no campo Requerente, no formato **CN = www.nomedosite.com.br**

Por exemplo, vejamos um site visitado pelo navegador Chrome. Se o CN do certificado instalado no site for idêntico à URL do próprio site, aparecerá um cadeado fechado no navegador, indicando que o certificado é legítimo e foi validado pela AC. Ou seja, o site é mesmo quem diz ser.



Caso o Certificado seja inválido, ou o site seja malicioso, o resultado é este:



52. O que é TLS? O que é SSL?

Resp.: - TLS é uma tecnologia chamada *Transport Layer Security*. Serve para garantir um canal seguro de comunicação na internet usando criptografia. A segurança da comunicação entre o FGC e as Instituições Financeiras é garantido por essa tecnologia. SSL é uma tecnologia mais antiga (*Secure Socket Layer*) que fazia a mesma coisa e foi substituída pelo TLS. Na prática os dois nomes se confundem.

Normalmente, a tecnologia TLS é empregada em websites e outros serviços (WhatsApp, FTP, Tinder, Uber etc) na Internet para aumentar a segurança das transmissões de dados. O Certificado Digital instalado em um dos computadores ou dispositivos participantes da conexão TLS serve basicamente para duas coisas:

- Validar a identidade e idoneidade do computador que tem o certificado (ou seja, "autenticar o servidor"), consultando uma Autoridade Certificadora (CA) e perguntando se ela conhece mesmo esse Certificado e seu dono.
- Após a autenticação, criar um canal de comunicação seguro e criptografado usando três chaves: a Pública, a Privada e uma terceira, negociada na hora.

53. O que é Mutual TLS Authentication?

Resp.: - É uma modalidade de autenticação TLS em que os dois participantes da conexão (e não apenas um, como é o usual) precisam ser autenticados por uma Autoridade Certificadora (CA). Para isso, os dois participantes precisam ter, cada um, seu próprio Certificado Digital. Além disso, em alguns casos, os dois participantes precisam estar conectados à Internet e ter o seu nome de DNS resolvido também publicamente na

Internet.

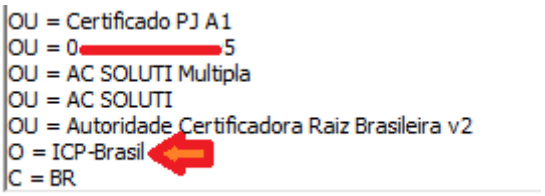
INFORMAÇÕES SOBRE OS CERTIFICADOS DA CADEIA ICP-BRASIL

54. O que é ICP Brasil?

Resp.: - A Infraestrutura Brasileira de Chaves Públicas – ICP-Brasil é uma PKI (ver definição neste FAQ) cuja Autoridade Certificadora Raiz – AC-Raiz é o ITI, do Instituto Nacional de Tecnologia da Informação (https://www.iti.gov.br), ligado à Casa Civil da Presidência da República.

55. Quando um certificado é considerado ICP-Brasil?

Resp.: - O Certificado Digital é considerado como pertencente à cadeia ICP Brasil quando sua Autoridade Certificadora (AC) Raiz é o ITI. Nesse caso, o identificador O do campo Emissor deve ser ICP-Brasil, e o identificador OU Raiz do Certificado é assinado pela Autoridade Certificadora Raiz Brasileira, conforme imagem.



56. Quanto tempo demora, em média, um certificado ICP-Brasil para ser emitido?

Resp.: - Cerca de um mês (30 dias ou mais). Como o Certificado Digital ICP-Brasil identifica oficialmente a empresa, uma série de documentos deve ser validada pela AC antes da emissão.

Lembramos que a **Circular 3.915/18** foi publicada em **outubro de 2018**, e que nosso manual técnico foi publicado em maio de 2019.

INSTRUÇÕES SOBRE OS CERTIFICADOS DIGITAIS USADOS NO CONTRIBUIÇÕES

57. Como o FGC usará o Certificado Digital no Censo e Contribuições?

Resp.: - No caso das entregas de Censo e Contribuições para o FGC, usaremos os Certificados Digitais para:

- O FGC verificar a autenticidade das Instituições Financeiras (IFs) pelo método **TLS Mutual**, por meio da verificação dos Certificados Digitais das IFs, impedindo que impostores mal-intencionados se passem por elas.
- O FGC usará o certificado também para verificar a identidade do computador (estação ou servidor) que transmitirá os arquivos do Contribuições.

- As IFs verificarem a autenticidade do FGC, por meio da verificação do Certificado Digital do FGC, impedindo que as IFs enviem as informações de Censo e Contribuições para impostores.
- Criar um canal criptografado TLS para proteger a transmissão (ver TLS/SSL).

58. O FGC indica, na seção 6.3, página 8 do Manual Operacional e Técnico do Censo, que os certificados precisam seguir a norma X.509. O que é X.509?

Resp.: - X.509 é uma norma que define a tecnologia de Certificados Digitais usados em implementações de Chave Pública na Internet. É uma das normas aceitas hoje para implementação de PKIs (*Public Key Infrastructures*).

É também a norma usada para a tecnologia TLS/SSL, que implementa conexões seguras na Internet baseadas em Certificado Digital. Os certificados enviados ao FGC devem todos ser aderentes à norma X.509.

59. O FGC indica, na seção 6.3, página 8 do Manual Operacional e Técnico, que os certificados precisam ser enviados no formato PEM. O que é um certificado PEM?

Resp.: - De forma simplificada, os Certificados Digitais podem ser codificados ou em formato binário (X.509 DER) ou em formato de texto puro ASCII Base64 (X.509 PEM).

Para o FGC, é necessário enviar os certificados em formato X.509 PEM.

Para identificar um arquivo PEM, basta abri-lo com um editor de textos (pode ser o Bloco de Notas / Notepad do Windows).

O texto deve começar com o marcador **BEGIN CERTIFICATE** e terminar com **END CERTIFICATE**.

Exemplo:

```
-----BEGIN CERTIFICATE-----
A1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2VydGlmaWNhdGUgYXV0aG9y
aXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdudVRMUyBjZXJ0aWZpY2F0
dGlmaWNhdGUgYXV0aG9yaXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdu
dVRMUyBjZXJ0aWZpY2F0ZSBhdXRob3JpdHkwWTATBgcqhkjOPQIBBggqhkjOPQMB
BwNCAARS2I0jiuNn14Y2sSALCX3IybqiIJUvxUpj+oNfzngvj/Niyv2394BWnW4X
SM49BAMCA0gAMEUCIDGuwD1KPyG+hRf88MeyMQcqOFZD0TbVleF+UsAGQ4enAiEA
ZpY2F0ZSBhdXRob3JpdHkwWTATBgcqhkjOPQIBBggqhkjOPQMBWZpY2FVQQIEWNh
l4wOuDwKQa+upc8GftXE2C//4mKANBC6It01gUaType=
-----END CERTIFICATE-----
```

Se não houver marcadores BEGIN e END no Certificado, não está em formato PEM e, portanto, não é válido para o FGC.

60. Meu certificado está com a extensão .PFX. Posso enviá-lo ao FGC?

Resp.: - NÃO. Arquivos .PFX, .P12, .P7B/.P7C, .JKS e .DER, apesar de também serem Certificados Digitais, não devem ser enviados ao FGC. Eles estão em formato binário (DER ou outros), que não é reconhecido pela API do FGC. Alguns desses arquivos podem conter a Chave Privada; essa chave nunca deve ser enviada ao FGC! Também não deve ser enviado o arquivo .KEY. Esse é o arquivo que contém a Chave Privada para os certificados PEM.

61. O certificado da Instituição Financeira, para uso no Contribuições, precisa obrigatoriamente validar um domínio ou URL?

Resp.: - DEPENDE. Por conta da criticidade e sigilo das informações enviadas pelos arquivos FGC405 e FGC406 do Contribuições, é necessário garantir e autenticar a identidade e a origem das conexões vindas das Instituições Financeiras (IFs) em direção à API do FGC.

A comunicação entre as Instituições Financeiras (IFs) e o FGC se dará por uma **API disponível publicamente na Internet** e, portanto, pode estar à mercê de impostores e ataques *Man-in-the-middle*. Por isso, optamos por uma autenticação TLS dupla (***Mutual TLS Authentication***), que usa Certificados Digitais nas duas pontas (IF e FGC). Dessa forma, o FGC tem certeza de que o interlocutor é a Instituição Financeira, e a IF tem certeza de que está falando com o FGC.

Portanto, temos três possibilidades:

- **Servidores diretamente conectados à internet, com IP válido próprio**: esses servidores estão mais expostos a ataques e por isso é desejável identificá-los pontualmente. Por isso, o certificado será validado pela Chave Pública, pela OU de identificação da propriedade do certificado e, também, pelo **FQDN** da máquina que iniciará a conexão com a API do FGC. Caso o servidor esteja atrás de proxy ou balanceador de carga, o certificado pode ser instalado nesses elementos de rede em vez dos servidores. O FQDN da máquina conectada diretamente à internet (os próprios servidores ou o balanceador/proxy) precisa ser resolvido por DNS público na Internet.

- **Estações de trabalho na rede corporativa, ou servidores sem conexão direta à internet (IP interno, via NAT)**: nesses casos, o computador (estação ou servidor) que rodará o sistema de envio está melhor protegido dentro da rede corporativa da IF. Portanto, o certificado será validado pela Chave Pública, pela OU de identificação da propriedade do certificado e, também, pelo domínio de DNS do website da empresa. **Não é necessário resolver o FQDN** individual desses computadores em DNS público, apenas o domínio, ou um FQDN fictício à escolha da IF. Por exemplo, se o site da IF é **www.bancoexemplo.com**, o CN pode ser (não limitados a esses exemplos):
  - **bancoexemplo.com**
  - **fgc.bancoexemplo.com**
  - **censo.bancoexemplo.com**
  - ou mesmo **www.bancoexemplo.com**

- **Estações de trabalho / servidores na rede corporativa com bloqueio à transmissão de certificados de cliente:** em algumas Instituições Financeiras, a infraestrutura de segurança (firewall, filtro de conteúdo) impede a transmissão de certificados de dentro para fora da rede corporativa. Nesse caso, **é necessário contactar a equipe de Suporte do Contribuições (**contribuicoes@fgc.org.br**) para alinhar uma solução técnica de contorno.** Como a verificação de credenciais é reduzida nesse caso, o FGC emitirá uma Carta de Risco à IF formalizando a exceção e responsabilizando a IF integralmente pelo risco.

62. Tenho dois (ou mais) servidores diretamente conectados à internet, com IPs válidos, que se conectarão à API do FGC. Eles podem usar o mesmo certificado?

Resp.: - DEPENDE. Se cada servidor responder por um FQDN diferente, cada servidor precisará de um certificado separado. Se todos os servidores estiverem atrás de um balanceador de carga ou um proxy, um certificado único pode ser instalado nesses elementos. A implementação exata varia caso a caso e depende da infraestrutura e das Políticas de Segurança da Instituição Financeira.

63. A aplicação que a Instituição Financeira desenvolveu é um aplicativo para Estações de Trabalho. Nossa rede corporativa está atrás de uma cadeia de proxies, e não temos acesso a eles. Nossa infraestrutura é gerenciada por equipes de TI em outros países. Como deve ser o Certificado Digital?

Resp.: - Nesses casos o procedimento padrão é:

- **Não é necessário resolver o FQDN** individual desses computadores em DNS público, apenas o domínio, ou um FQDN fictício à escolha da IF. Por exemplo, se o site da IF é **www.bancoexemplo.com**, o CN pode ser (não limitados a esses exemplos):
  - **bancoexemplo.com**
  - **fgc.bancoexemplo.com**
  - **censo.bancoexemplo.com**
  - ou mesmo **www.bancoexemplo.com**

- Caso a comunicação não funcione, devido a restrições internas de segurança da IF, entrar em contato com o Suporte Técnico do Contribuições (contribuicoes@fgc.org.br) para informar a situação de exceção. É aconselhável testar se há mesmo um problema (às vezes o problema não se apresenta, mesmo com as restrições).

ATENÇÃO: qualquer solução de contorno acordada entre a IF e o FGC será documentada e o risco deverá ser assumido pela IF com uma Carta de Risco. Essa solução de contorno será **provisória**, terá prazo para ser revogada e a IF deverá usar esse prazo para implementar a solução definitiva de acordo com a arquitetura base proposta pelo FGC. O FGC pode arbitrariamente recusar o risco, a seu critério e após análise, e nesse caso a IF deverá tomar providências para atender minimamente aos requisitos técnicos da API proposta.

64. A solução de contorno, citada nos casos acima, poderá ser adotada permanentemente?

Resp.: - NÃO. O FGC dará um prazo razoável para que a Instituição Financeira possa adequar sua infraestrutura de forma a conectar-se à API do Contribuições no modelo proposto – a saber, conexão via internet à API do FGC com autenticação TLS Mutual e validação do Certificado Digital dentro da mensagem JSON.

65. Posso resolver o FQDN da minha máquina com um DNS interno na minha rede corporativa, para fins de autenticação do certificado?

Resp.: - NÃO, e nem é necessário. O nome de DNS da máquina que se conecta ao FGC só precisa ser resolvido na Internet quando a máquina estiver conectada diretamente na Internet (i.e. possuir um IP válido).

Em qualquer outro caso, o CN do Certificado Digital deve conter o domínio principal da IF (i.e., se o site da IF é **www.bancoexemplo.com**, o domínio é **bancoexemplo.com**) ou um FQDN fictício (por exemplo, **fgcs.bancoexemplo.com**). Caso haja problemas (e somente se houver problemas) teremos que aplicar uma solução de contorno, conforme

a pergunta anterior. Os problemas encontrados devem ser resolvidos caso a caso.

Contacte o Suporte Técnico do Contribuições para obter orientação: contribuicoes@fgc.org.br.

66. O FGC exige que o Certificado Digital usado nos sistemas Censo e Contribuições de **Produção** seja integrante da cadeia ICP Brasil?

Resp.: - SIM. O Certificado Digital a ser usado no Censo e Contribuições tem que pertencer à cadeia ICP Brasil, mas apenas para o ambiente de **Produção**.

O Certificado ICP-Brasil pode ser emitido por qualquer AR credenciada pelo ITI. O site do ITI tem uma lista de ACs aptas a emitir certificados ICP-Brasil, e a partir delas é possível encontrar uma AR próxima da Instituição Financeira.

Para consultar a lista das autoridades certificadoras, acesse o site:

https://estrutura.iti.gov.br/

É importante que a AR seja na mesma cidade da Instituição Financeira, pois haverá validação presencial da documentação da IF e dos Responsáveis Legais.

Para **Homologação**, o Certificado pode ser auto assinado (i.e., emitido pela própria Instituição Financeira), não precisa ser ICP-Brasil nem ser adquirido de uma AR.

67. Não deu tempo de adquirir um Certificado Digital ICP-Brasil, e o prazo para entrada em produção está se esgotando. Posso usar um certificado comum, emitido por uma CA reconhecida, mas fora do ICP-Brasil?

Resp.: - NÃO.

68. O Certificado Digital da instituição pode ter validade de 3 anos? Qual o procedimento de renovação?

Resp.: - NÃO. O Certificado Digital, tanto de homologação como de produção, deve ter **validade de um (01) ano**. Certificados com validade diferente de um ano serão rejeitados.

Desde abril de 2021, todos os certificados digitais da Cadeia ICP-Brasil possuem validade de 1 ano, apenas. É impossível emitir Certificados ICP-Brasil com outras validades. Caso a emissão com validade maior volte a ser possível no futuro, ainda assim o FGC aceitará apenas Certificados ICP-Brasil com validade de um ano.

Os Certificados Digitais já renovados devem ser cadastrados FGC com antecedência de **30 dias antes do vencimento** do anterior, para evitar interrupção de operação.

Os Certificados Digitais devem ser enviados para o e-mail contribuicoes@fgc.org.br.

69. O que é preciso colocar no **CSR** para gerar um certificado válido para o FGC?

Resp.: - Critérios comuns a todas as IFs:

- Certificado deve pertencer à cadeia ICP Brasil
- Certificado deve ser válido para autenticação SSL de servidores, ou seja, a destinação do certificado deve ser:
  - Garante a identidade de um computador remoto
  - Prova a sua identidade para um computador remoto
- Validade de um (01) ano.
- No campo **Requerente**:
  - OU: Raiz do CNPJ
  - OU: CNPJ completo
  - O: Nome da IF (Razão Social **exata**)
  - C: BR
  - S (Estado) e L (Cidade/Localidade) são opcionais, mas se forem usados devem ser válidos e no Brasil.
  - CN: conforme critérios a seguir.

Servidores com acesso direto à internet (i.e. possui IP válido):

CN: FQDN da máquina que origina a conexão imediata com o FGC (i.e., servidor, balanceador de carga, proxy etc)

Estações de trabalho ou servidores em rede corporativa:

CN: Não é necessário resolver o FQDN, apenas o domínio, ou um FQDN fictício à escolha da IF. Por exemplo, se o site da IF é www.bancoexemplo.com, o CN pode ser (não limitados a esses exemplos):

- bancoexemplo.com
- fgc.bancoexemplo.com
- censo.bancoexemplo.com
- ou mesmo www.bancoexemplo.com

Estações de trabalho ou servidores em rede corporativa e sem possibilidade de transmissão do certificado (i.e. restrições de segurança)**:**

- CN: Domínio DNS da IF ou FQDN fictício (conforme item anterior)
- Necessária solução de contorno – contactar contribuicoes@fgc.org.br. O FGC analisará a situação e decidirá se o risco pode ou não ser aceito. O FGC tem a

última palavra para arbitrar se uma situação de risco é aceitável ou para rejeitá-la. Será emitida ressalva em **Carta de Risco** para documentar a exceção, caso aprovada.

70. Já adquiri um certificado ICP-Brasil e percebi que não atende às exigências do FGC. Posso usar esse certificado?

Resp.: - TALVEZ. Verifique o certificado usando o seguinte *checklist*:

- É ICP-Brasil mesmo?
- Identifica a Instituição Financeira (IF) de alguma forma (Razão Social ou CNPJ)?
- É válido como autenticador de computador (certificado SSL)?

Se a resposta a pelo menos uma das três perguntas for **não**, a IF deverá reemitir o certificado ICP Brasil obedecendo fielmente ao exposto na pergunta anterior. Se a resposta a todas as três perguntas for **sim**, envie o arquivo do certificado (com extensão .TXT) para o FGC pelo e-mail contribuicoes@fgc.org.br. A equipe técnica do Contribuições avaliará o Certificado e informará se pode ser usado.

Observe que, desde abril de 2021, todos os certificados digitais da Cadeia ICP-Brasil atendem completamente às exigências do FGC. Se você adquiriu um Certificado ICP-Brasil após essa data, mesmo que para outra finalidade, provavelmente servirá.

71. Já tenho o certificado correto. Como envio para o FGC?

Resp.: - Antes de enviar, verifique se realmente o Certificado Digital que você tem em mãos obedece aos seguintes padrões e formatos:

- Aderente à norma X.509.
- Formato PEM (texto ASCII) codificado em Base64.
- Contém todas as informações solicitadas e de forma correta, conforme as perguntas anteriores.

Os meios de envio são:

- **Cadastro Técnico**: enviado ao FGC pelo e-mail contribuicoes@fgc.org.br; o arquivo que contém o certificado deve ser anexado com a extensão **TXT** para termos acesso ao conteúdo de texto.
- **Portal do Desenvolvedor (ainda não divulgado)**: copiar (Ctrl+C) o trecho entre BEGIN CERTIFICATE e END CERTIFICATE dentro do arquivo PEM e colar

(Ctrl+V) no Portal. Caso o Portal do Desenvolvedor esteja indisponível, enviar o certificado pelo e-mail do cadastro técnico, contribuicoes@fgc.org.br.

72. Meu Certificado Digital já está cadastrado no FGC. Preciso fazer mais alguma coisa?

Resp.: - SIM. Em operação normal, para a transmissão e entrega dos arquivos FGC300 e FGC301, o trecho entre BEGIN CERTIFICATE e END CERTIFICATE deve ser transmitido no campo "x-client-certificate" do *header* da mensagem JSON.

Consulte a documentação do seu sistema de envio do Censo ou Contribuições para saber onde inserir seu Certificado.

73. Para o ambiente de produção: A dúvida é se podemos utilizar o mesmo certificado Digital utilizado no SPB, pois, após analise identificamos que contenha as exigências necessárias mencionadas no Manual Operacional Técnico. Em caso positivo, podemos encaminhar o arquivo B64 (Base 64) para cadastro?

Resp.: - SIM. Mas é preciso conferi-lo para ter certeza. Consulte as perguntas anteriores para verificar se o certificado pode ser usado.

74. A máquina que vai transmitir os arquivos do Contribuições e informações referentes a contribuições precisa estar conectada diretamente à Internet?

Resp.: - NÃO. Ela pode estar atrás de um firewall, de um balanceador de carga ou de um proxy, ou de outros *appliances* de segurança. A máquina pode ser tanto um servidor como uma estação de trabalho.

Entretanto, existem dois cenários:

- Servidores com acesso direto à internet
- Estações de trabalho ou servidores sem acesso direto à internet (i.e. atrás de proxy ou outro elemento de segurança)

Para cada situação, a implementação (e o certificado utilizado) muda um pouco. Consulte as perguntas anteriores para mais informações.

75. A máquina que vai transmitir os arquivos do Contribuições e informações referentes a contribuições precisa ter seu nome publicamente resolvido por um DNS na Internet?

Resp.: - DEPENDE.

É obrigatório resolver o nome de DNS da máquina que hospeda o sistema da Instituição

Financeira caso ela esteja diretamente conectada à Internet (i.e. possua um IP válido).

Caso a máquina esteja dentro de uma rede corporativa, acessando a Internet protegida por proxy, firewall, NAT etc, consulte as perguntas anteriores.