

PDS - Certificado Corporativa - Perguntas Frequentes (FAQ)

Perguntas Frequentes (FAQ) sobre o Certificado Corporativa

ICPEdu - Infraestrutura de Chaves Públicas para Ensino e Pesquisa

i Aqui você encontra perguntas e respostas para as principais dúvidas e questionamentos feitos pelas instituições cliente da RNP sobre a modalidade Certificado Corporativa da ICPEdu.

Caso sua dúvida não seja respondida aqui, na [página oficial do serviço](#), ou na [página do serviço na wiki](#) da RNP, favor enviá-la para atendimento@icp.edu.br com o assunto **Certificado Corporativa**.

Para obter mais informações sobre como operar o portal web do Certificado Corporativa, [clique aqui](#).

1) O que é o Certificado Corporativa?

A Certificado Corporativa é uma das modalidades da Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu) e disponibiliza meios para que as instituições cliente desta modalidade emitam certificados SSL com a cadeia de certificação publicada automaticamente nos principais browsers e aplicativos comerciais, assim, eliminando a famosa mensagem "Esta conexão não é confiável".

Para possibilitar a emissão de certificados com estas características, foi fechado um acordo entre a RNP e a GlobalSign onde RNP é responsável por ofertar o serviço de forma mais simplificada, menos burocratizada possível e gratuita, tendo a GlobalSign como um parceiro chave na prestação deste serviço.

2) Pra que preciso de certificados SSL automaticamente reconhecido pelos browsers?

Certificados SSL são comumente utilizados em servidores de hospedagem web para proteção de sites através da criptografia da comunicação entre cliente e servidor, além de ser uma garantia a mais de que a página realmente pertence a quem ela diz pertencer, ou seja, é questão de segurança básica o uso de certificados SSL.

Se você se encaixa em algum dos casos abaixo, você definitivamente precisa aderir ao serviço de Certificado Corporativa da ICPEdu:

- Você precisa garantir a segurança dos seus serviços de email ou similares;
- Você precisa garantir a segurança dos seus serviços web com autenticação e área restrita (usuário e senha);
- Você precisa garantir a segurança dos dados transportados entre cliente e servidor (pois eles são privados ou confidenciais);
- Você precisa passar mais credibilidade e profissionalismo aos seus usuários e parceiros?

Se acessamos uma página web e temos a mensagem "Esta conexão não é confiável" (imagem abaixo), ela tira um pouco da credibilidade daquela página além de acender uma fagulha de desconfiança pois aquele site pode ter sido comprometido, não ser de fato quem ele diz ser ou foi mesmo descuido e descaso da equipe técnica que fez uso de um certificado auto-assinado, que qualquer um pode criar um igual. Se você não quer que esta impressão seja passada aos usuários dos seus serviços web, você definitivamente precisa aderir ao serviço de Certificado Corporativa da ICPEdu.

3) Como funciona o serviço?

No documento de adesão a esta modalidade o reitor ou representante máximo da instituição/organização deverá apontar um responsável pela instituição frente ao serviço, após concluir o processo de adesão este responsável receberá as credenciais de acesso ao portal de gerenciamento de certificados por e-mail, por medidas de segurança, **o primeiro passo deve ser alterar a senha de acesso ao portal.**

- O portal poderá ser acessado através do endereço corporativo.icpedu.rnp.br.
- Os manuais e instruções de uso do portal podem ser acessados aqui: [AC SSL Corporativa - Instruções de uso](#).

Tudo referente ao gerenciamento dos certificados é feito diretamente no portal web pelo responsável ou técnicos da instituição. O portal permite que os usuários façam a emissão, reemissão (ou renovação) e revogação de certificados para todos os domínios sob a responsabilidade da instituição, nenhuma destas ações envolvem a RNP ou a GlobalSign, todas são executadas diretamente pelos usuários.

Vale ressaltar que somente é permitida a emissão de certificados para os domínios comprovadamente sob a responsabilidade da instituição.

Cada instituição pode ter no máximo 3 usuários simultâneos no portal web, contabilizando o responsável.

4) Quais os requisitos para minha instituição aderir?

O único pré-requisito para adesão a esta modalidade da ICPEdu é a instituição ser credenciada a utilizar os serviços da RNP, ou seja, se a instituição já utiliza algum dos serviços da RNP ela pode iniciar o processo de adesão seguindo estes passos: [Certificado Corporativa - Adesão](#)

Caso a instituição não seja credenciada a utilizar os serviços da RNP, o processo de credenciamento pode ser iniciado através do e-mail rc@rnp.br.

Nenhum outro pré-requisito é necessário para adesão ao serviço assim como não é necessária a aquisição de equipamentos e nem adequação da infra por parte da instituição, toda infra necessária é fornecida pela RNP.

5) Qual o custo de adesão e uso do serviço para a minha instituição?

Não existe custo na adesão e no uso da modalidade Certificado Corporativa da ICPEdu para instituições credenciadas da RNP, todos os custos são absorvidos pela a RNP e não são repassados aos clientes.

Mais informações sobre o processo de adesão, [clique aqui](#).

6) Como faço para aderir a modalidade de Certificado Corporativa?

[Clique aqui](#) para mais informações sobre como funciona o processo de adesão da Certificado Corporativa.

7) Qual o custo para emissão de certificados?

Não existe custo para as instituições credenciadas da RNP, todos os custos são absorvidos pela a RNP e não são repassados aos clientes, sendo assim, a emissão de certificados é totalmente gratuita para as instituições.

8) Quantos certificados posso emitir?

A emissão de certificados nesta modalidade é ilimitada.

A parceria entre a RNP e GlobalSign contempla a emissão de um número ilimitado de certificados, se a instituição emitir 1 certificado ou 1000 certificados o valor pago pela RNP será o mesmo, quanto mais certificados forem emitidos melhor.

9) Posso emitir certificados para qualquer domínio?

Não, cada instituição poderá emitir certificados somente para domínios, e seus respectivos subdomínios, registrados em nome da própria instituição ou daqueles que ela é comprovadamente a responsável por manter.

Domínios de terceiros não serão habilitados para emissão de certificados.

10) Quais as características dos certificados que posso emitir?

A modalidade Certificado Corporativa da ICPEdu permite a emissão de certificados SSL comumente utilizados em servidores para proteção de websites através de criptografia dos dados e consequentemente a privacidade destes dados.

Esta modalidade permite a emissão de certificados SSL com validade de 1, 2 ou 3 anos, estes podendo ser de dois tipos distintos:

Standard SSL: É o certificado SSL padrão emitido para proteger um domínio ou subdomínio específico, por exemplo [wiki.rnp.br](#), [mail.rnp.br](#) e [mconf.rnp.br](#). O Standard SSL normalmente protege um domínio específico (também chamado de CN e Common Name), no entanto, quando houver a necessidade de se proteger mais de um domínio ou subdomínio recomenda-se o uso de **SANs (Subject Alternative Names)**, para saber mais sobre SANs [clique aqui](#).

Wildcard SSL: É o certificados emitido para proteger todos subdomínios de primeiro nível de um determinado domínio, o wildcard [*.rnp.br](#), por exemplo, está apto a proteger todos os subdomínios de primeiro nível de [rnp.br](#) como [wiki.rnp.br](#), [mail.rnp.br](#) e [primeiro.rnp.br](#), mas não protege o próprio domínio [rnp.br](#) e nem domínios de segundo, terceiro ou mais níveis como [segundo.primeiro.rnp.br](#), [www.mail.rnp.br](#) e [www.wiki.rnp.br](#). [Clique aqui para entender mais sobre certificados wildcard](#).



Por questões de segurança **o uso de certificados wildcard não é recomendado**, embora em alguns cenários e ambientes ele é a única solução.

Recomendamos que sempre que possível substituir o uso de certificados wildcard por Standard SSL + **SANs (Subject Alternative Names)**, para saber mais sobre SANs [clique aqui](#).

11) Posso emitir certificados Wildcard?

Sim, a emissão de certificados Wildcard também está disponível nesta modalidade, sem custo e sem limite no número de certificados a serem emitidos.

Vale lembrar que certificados wildcard protegem apenas subdomínios de primeiro nível, por exemplo, o wildcard [*.rnp.br](#) está apto a proteger todos os subdomínios de primeiro nível de [rnp.br](#) como [wiki.rnp.br](#), [mail.rnp.br](#) e [primeiro.rnp.br](#), mas não protege o próprio domínio [rnp.br](#) e nem domínios de segundo, terceiro ou mais níveis como [segundo.primeiro.rnp.br](#), [www.mail.rnp.br](#) e [www.wiki.rnp.br](#).

Para entender mais sobre certificados wildcard, [clique aqui](#).



Por questões de segurança **o uso de certificados wildcard não é recomendado**, embora em alguns cenários e ambientes ele é a única solução.

Recomendamos que sempre que possível substituir o uso de certificados wildcard por Standard SSL + **SANs (Subject Alternative Names)**, para saber mais sobre SANs [clique aqui](#).

12) Como emitir um certificado para vários domínios sem utilizar um certificado wildcard?

O uso de certificados wildcard pode aumentar os riscos à segurança dos seus servidores, [clique aqui para entender mais sobre certificados wildcard](#).

Como uma solução para esta questão temos a opção de emitir certificados para uma lista de domínios e subdomínios, com no máximo 100 domínios e subdomínios, solução esta chamada de Subject Alternative Names, ou simplesmente SAN's, para saber mais sobre **SANs** e aprender como emitir certificados Standard para vários domínios, [clique aqui](#).

13) Quais tipos de certificados estão incluídos no serviço e quais não estão?

A Certificado Corporativa tem como objetivo o fornecimento de certificados SSL automaticamente reconhecidos nos principais browsers e aplicativos comerciais, todos os certificados SSL (Standard e **Wildcard**) emitidos já são contemplados no acordo/contrato firmado entre a RNP e a GlobalSign, no entanto, o acordo contempla apenas os certificados SSL e não outros tipos de certificados como aqueles destinados a assinatura de código fonte e certificados pessoais para assinatura de documentos ou e-mails. (Para saber mais sobre emissão de certificados pessoais entenda como funciona a modalidade [AC Pessoas da ICPEdu](#)).

Certificados SSL são mais comumente utilizados em servidores que hospedam páginas web como serviços de e-mail e portais que possuam qualquer tipo de dados que precisem de proteção e criptográfica da comunicação entre cliente e servidor.

Em resumo, a Certificado Corporativa contempla exclusivamente os certificados emitidos através da aba Managed SSL do portal web, se você tem necessidade de emissão de algum outro tipo de certificado, favor entrar em contato conosco através do e-mail atendimento@icp.edu.br.



Dúvidas, críticas ou sugestões

Quer **aderir** a modalidade Certificado Corporativa? [Clique aqui](#) e entenda o **processo de adesão**.

Quer entender como **operar o portal web** da modalidade Certificado Corporativa? [Clique aqui](#) e acesso nossos **manuais e instruções de uso**.

Quer aprender mais sobre certificados **wildcard**? [Clique aqui](#).

Quer aprender mais sobre certificados com **Subject Alternative Names (SAN's)**? [Clique aqui](#).

Acesso o **site oficial** do serviço [clikando aqui](#).

atendimento@icp.edu.br



Service Desk RNP

Telefones: +55 (61) 3243-4330

Fone@RNP: (61) 1030-3001 e (61) 1030-3002

E-mail: sd@rnp.br

O horário de atendimento do Service Desk é das 08:00 as 22:00 todos os dias.