

Manual SSL - Certificado segurança do site - Deixar site (domínio próprio) seguro

Um certificado de segurança em um site é um tipo de tecnologia que ajuda a proteger as informações e dados transmitidos entre o usuário e o site, evitando que sejam interceptados por terceiros.

O certificado de segurança é **emitido por uma Autoridade Certificadora (AC)**, que verifica a identidade do proprietário do site e a integridade do conteúdo oferecido. A AC **emite um certificado digital**, que é **instalado no servidor do site** e, em seguida, é usado para **criptografar as informações que são trocadas entre o site e o usuário**.

A presença de um certificado de segurança pode ser identificada pela existência do "**cadeado**" na barra de endereço do navegador, bem como pelo uso do protocolo "https" em vez de "http". Isso significa que a comunicação entre o navegador e o servidor é criptografada e, portanto, **mais segura**.

Além disso, ter um certificado de segurança também pode aumentar a confiança do usuário no site e na marca, o que pode resultar em mais conversões e fidelidade do cliente.

Existem diferentes tipos de certificados de segurança, incluindo:

Certificado de validação de domínio (DV): verifica apenas se o proprietário do site possui controle sobre o domínio. É o tipo mais básico de certificado de segurança.

Certificado de validação organizacional (OV): verifica se a organização proprietária do site é legítima e está registrada.

Certificado de validação estendida (EV): verifica se a organização proprietária do site é legítima e está registrada, além de fornecer informações adicionais sobre a empresa, como nome e localização.

Os certificados de segurança precisam ser renovados periodicamente, para garantir que a criptografia continue sendo eficaz e que o site continue protegido. É importante que os usuários verifiquem se um site possui um certificado de segurança antes de inserir informações pessoais ou confidenciais, como senhas ou números de cartão de crédito.

Abaixo fizemos um passo a passo para auxiliar o processo de geração de um certificado para o seu site:

- Se você não possui, **adquira um domínio próprio** e **aponte o DNS** do domínio para o **PROMAD**;
 - **Compre** um certificado junto a uma **AC**;
 - Caso seja necessário a validação do domínio e o DNS de seu site esteja apontado para a estrutura do PROMAD, escolha a opção de validação por DNS. Nesse ponto mande para nossa central as instruções que o site da AC disponibiliza para melhor auxiliarmos;
 - Se o site da AC não gerar um arquivo de CSR, solicite a nossa central que gere um arquivo CSR e lhe envie;
 - Com o arquivo CSR em mãos, siga o passo-a-passo disponibilizado pela AC para finalizar a geração do certificado;
- Para instalarmos o certificado em seu site, precisamos que nos envie os arquivos abaixo:
 - **arquivo com a extensão .crt;**
 - **arquivo com a extensão .ca;**
 - **arquivo com a extensão .key (não é necessário envio se nossa equipe gerou o arquivo CSR);**

Revision #2

Created 5 July 2023 17:27:20 by Admin

Updated 13 December 2023 17:39:46 by Admin