CERTIFICAÇAO DIGITAL - SSL

O certificado SSL (Secure Socket Layer) certifica servidores, sites ou aplicações permitindo ao usuário final conferir a autenticidade do site em que navega e comunicar-se por meio de um canal seguro e protegido (baseado em SSL) utilizando tecnologia de criptografia.

Prodesp

GOVERNO DO ESTADO DE SÃO PAULO

CARACTERÍSTICAS BÁSICAS

- ✓ Protege e autentica servidores e sites públicos e internos;
- ✓ Selo de conformidade internacional WebTrust;Segurança
- ✓ Segurança sinalizada pelo cadeado fechado exibido em todos os navegadores e o protocolo “https” no endereço do site;
- ✓ Melhora o ranqueamento do site nos mecanismos de busca de navegadores (Google);
- ✓ Para certificados de Raiz Internacional:
    - Validação Organizacional (OV): que dá maior credibilidade ao site, pois valida a empresa detentora daquele endereço de URL/site;
    - Garantia de até U$$ 1,25 milhão (seguro), por certificado, para cobertura de riscos em caso de perda causada por um erro no processo de identificação, de declarações falsas no certificado, risco de perda/extravio de documentos relacionados ao processo de identificação que um requerente ainda contra erros intencionais ou acidentais introduzidos em um Certificado;
    - O acionamento do seguro deverá a ser realizado diretamente à AC Raiz Internacional, conforme estabelecido na política de garantia da AC Globalsign, disponível no endereço https://www.globalsign.com/en/repository/globalsign-warranty-policy.pdf
- ✓ Compatível com todos os principais navegadores e dispositivos móveis;
- ✓ Aderente às exigências do CA/B Fórum (CA Browser é o fórum das empresas fabricantes de software de navegadores da internet e autoridades de certificadoras). O CA/B Fórum publica requisitos básicos para a emissão e gerenciamento de certificados publicamente confiáveis, sendo os requisitos que uma autoridade de certificação deve atender para emitir certificados digitais para servidores SSL / TLS para serem publicamente confiáveis pelos navegadores.

- ✓ Aderente aos requisitos de Certificate Transparency (CT), exigidos por navegadores do mercado;

Certificados SSL

- ✓ **SSL WildCard**
  - Conhecido como certificado curinga, é um certificado que protege uma quantidade ilimitada de subdomínios de um ou mais domínios com um único certificado;
    - É emitido para *.seudomínio.com, onde o asterisco representa todos os subdomínios possíveis;
- ✓ **SSL Standard - OV**
  - Verifica a identidade da organização (por exemplo, uma empresa sem fins lucrativos ou organização governamental) do candidato ao certificado. Os certificados OV são frequentemente usados por corporações, governos e outras entidades que desejam fornecer uma camada extra de confiança a seus visitantes;
- ✓ **SSL Codesign**
  - É utilizado por programadores em todas as plataformas para assinar digitalmente os aplicativos e softwares que são distribuídos na internet. Incluindo o nome do desenvolvedor e protegendo contra injeções de malware e outros tipos de corrupção;

BENEFÍCIOS

- ✓ Aumento da relação de confiança;
- ✓ Redução da possibilidade de fraude;

Portfólio

- ✓ Mais segurança de dados;
- ✓ Dados analíticos mais apurados;
- ✓ Melhores práticas de segurança operacional;
- ✓ Melhor posicionamento da página no Google

PRÉ-REQUISITOS

- ✓ Validação da organização para a confirmação da propriedade do domínio a ser certificado;
- ✓ Validação de informações do proprietário (ex.: nome e endereço) que são autenticados.