Recomendação de Segurança 002/2018 - Cogetic/VPGDI

Em 31 de outubro de 2018

Para: Gestores de TI das unidades da Fiocruz

Assunto: Recomendação do uso de certificados SSL

Sobre o protocolo SSL/TLS

O protocolo SSL (*Secure Sockets Layer*) e o seu sucessor o TLS *(Segurança da Camada de Transporte)*, são protocolos de criptografia projetados para a Internet e fornecem privacidade e integridade nas comunicações entre um cliente e uma aplicação Web, executando a troca de informações dentro de um canal seguro.

Com o crescimento e popularidade da Internet, inclusive na Administração Pública Federal – APF, aumenta também a quantidade de serviços oferecidos em meio digital e a necessidade de adoção de certificados SSL/TLS para garantir a autenticidade e a integridade dos sites.

Recomendações

Recomenda-se a adoção de certificados SSL em sítios dos órgãos da APF nas seguintes situações:

- Adotar certificados SSL em todas as páginas que lidem com dados sensíveis, devendo trafegar em páginas conhecidas como “conexão segura”, ou seja, as que usam o protocolo HTTPS.
- Utilizar certificados de Autoridades Certificadoras reconhecidas nacionalmente e internacionalmente.
- Utilizar sempre o protocolo TLS em uma aplicação que receba dados de usuários e senhas.
- Utilizar obrigatoriamente o protocolo TLS preferencialmente na versão 1.3.
- Devido a quantidade de vulnerabilidades existentes no protocolo SSL, recomendamos atualizar as versões antigas do protocolo do SSL para o

protocolo TLS (Isso é aplicado por meio da alteração da configuração de seu Webserver).

Referências

— http://dsic.planalto.gov.br/legislacao/RequisitosMnimosSIparaAPF.pdf

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações