Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Alerta de Segurança 003/2020 - Cogetic

Em 6 de julho de 2020

Para: Gestores de TI das unidades da Fiocruz

Assunto: Correção de vulnerabilidade nos certificados SSL

Prezados Gestores de TI,

Fomos notificados pela Rede Nacional de Ensino e Pesquisa – RNP sobre vulnerabilidade identificada nos certificados SSL corporativos emitidos através Infraestrutura de Chaves Públicas para Ensino e Pesquisa – ICPEdu.

Apesar de nenhum incidente ter sido registrado, alertamos sobre a revogação dos automática dos certificados atuais em 8/7/2020 e a necessidade de emissão de novos certificados em substituição aos anteriores. A expectativa é que a partir de 7/7/2020 já possamos emitir novos certificados com a vulnerabilidade corrigida.

Devido ao alto volume de certificados a serem emitidos e a fim de evitar transtornos motivados pelo uso de certificados revogados, pedimos que todas as unidades adotem imediatamente o seguinte procedimento:

1. Submeter solicitação de certificados através da RSI (https://rsi.fiocruz.br) através da opção: Segurança da Informação | Certificado Digital | Emissão de certificado digital SSL;
2. Anexar o arquivo .CSR correspondente ao *common name* do site que receberá o certificado;
3. Caso o site utilize nomes alternativos (conhecido como SAN), utilize o campo de descrição da RSI para listar esses nomes.

Notas:

1. O nome alternativo se refere as diferentes URL's que podem ser utilizadas para acessar um mesmo site (conteúdo/destino). Exemplo: *unidade*.fiocruz.br | www.*unidade*.fiocruz.br | portal.*unidade*.fiocruz.br;

2. No caso de sites com SAN, basta gerar o arquivo .CSR de um dos *common name* pelo qual o site responde e descrever os nomes alternativos diretamente na RSI. É imprescindível informar os nomes alternativos no campo de descrição da requisição da RSI, pois o sistema não lê essas informações diretamente no arquivo .CSR;
3. Não serão gerados certificados do tipo *wildcard*;
4. Orientações sobre a geração dos arquivos .CSR:
    - Utilizando o OpenSSL: https://video.rnp.br/portal/video?identificator=CSRICPEdu
    - Outros métodos: https://support.globalsign.com/ssl/ssl-certificates-installation/certificate-signing-request-csr-overview
5. Para facilitar a conferência dos certificados, será disponibilizada uma planilha com os *common name* de certificados vigentes.

Coordenação-Geral de Gestão de Tecnologia da Informação
Serviço de Segurança da Informação e Comunicações