INSTITUTO EVANDRO CHAGAS
MS-SECRETARIA DE VIGILÂNCIA EM SAÚDE

Utilização da Rede de Comunicação de Dados do IEC (RCD-IEC)

Objetivo

Estabelecer as normas de utilização dos recursos Rede de Comunicação de Dados do IEC (RCD-IEC) que englobam login na rede, manutenção de arquivos no servidor, tentativas não autorizadas de acesso, alteração de configurações e permissões locais nos computadores.

Abrangência

Esta norma deverá ser aplicada a todos os usuários do Instituto Evandro Chagas que utilizam os recursos de Tecnologia da Informação e Comunicação.

a) A solicitação de criação ou encerramento de conta de usuário da rede deve ser feita através de memorando padrão (modelo anexo ao documento), devidamente assinado pelo Chefe Imediato e dirigido ao Serviço de Administração que encaminhará a solicitação ao Setor de Informática;

b) Não serão permitidas tentativas de obter acesso não autorizado, tais como: tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor de rede (computador), rede ou conta; acesso aos dados não disponíveis para o usuário; conectar-se ao servidor de rede ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;

c) Não serão permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor de rede ou rede de dados.

- Isso inclui ataques do tipo DOS (*Denial of Service – Negação de serviço*), que visem a provocar congestionamento na rede e/ou tentativas deliberadas de sobrecarregar/invadir um servidor;

d) Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários, salvo casos para suporte técnico;

e) Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e se possível efetuar o *log off* da rede ou bloqueio da estação de trabalho através de senha quando a ausência não for se prolongar por muito tempo;

f) A manutenção de arquivos em diretórios pessoais é obrigatória a fim de evitar o acúmulo de arquivos inúteis bem como o de facilitar o backup dos dados do usuário quando necessário;

g) Material de natureza pornográfica e/ou discriminatória (audiovisual ou textual), não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da Rede de Comunicação de Dados do IEC (RCD-IEC);

h) Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário que possam comprometer o desempenho e funcionamento dos sistemas;

i) Pastas que podem ser acessadas por todos os usuários (pastas públicas) não deverão ser utilizadas para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível;

j) É obrigatório armazenar os arquivos inerentes ao Instituto Evandro Chagas no servidor de arquivos para garantir o backup e a alta disponibilidade destes;

k) Arquivos de caráter particular (fotos, músicas, vídeos, outros) são de responsabilidade do usuário e não poderão ser armazenados no servidor de arquivos;

l) Haverá limpeza semanal dos arquivos armazenados nas pastas públicas, para que não haja acúmulo desnecessário de arquivos;

m) É proibida a instalação ou remoção de softwares que não forem devidamente acompanhadas pelo SOINF, por meio de solicitação via e-mail para cs@iec.pa.gov.br ou ramal 5100 ou externo 3214-2204;

n) É vedada a abertura de computadores conectados na RCD para qualquer tipo de reparo. Caso seja necessário, o reparo deverá ocorrer pelo SOINF excetos os conectados em equipamentos laboratoriais;

o) Não será permitida a alteração das configurações de rede, exceto as executadas pelo SOINF por meio do suporte técnico, bem como modificações que possam trazer algum problema futuro;

p) É obrigatória a solicitação de desativação de conta de rede do funcionário em caso de desligamento. Deve-se enviar a solicitação de desligamento para cs@iec.pa.gov.br;

q) É proibido o uso de permissão local nos computadores (administrador local no computador), pois através desta permissão o usuário tem acesso total ao computador e pode instalar programas não licenciados, instalar vírus e programas espiões, além de executar outras atividades que comprometeriam a segurança da rede lógica.