NORMAS DE SEGURANÇA PARA CONTROLE DE ACESSO REMOTO

1. OBJETIVO:

Esta norma de segurança tem por objetivo definir critérios de segurança e descrever as ações para efetuar o acesso remoto no âmbito da Rede Corporativa do Ministério da Saúde.

2. APLICAÇÃO:

Esta norma de segurança se aplica ao Ministério da Saúde.

3. DOCUMENTOS DE REFERÊNCIA:

I - Norma NBR ISO/IEC 27000 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos - Requisito 6.0;
II - Norma NBR ISOIEC 17799 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a Gestão da Segurança da Informação;
III - Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
IV - Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;
V - Política de Segurança da Informação do Ministério da Saúde.

4. DEFINIÇÕES E SIGLAS:

Além das definições e siglas listadas a seguir, também são adotadas as definições contidas no documento da Política de Segurança da Informação e Comunicações do Ministério da Saúde.
I - CIINFO/MS: Comitê de Informação e Informática em Saúde;
II - DATASUS: Departamento de Informática do SUS;
III - Logs: Termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional;
IV - Rede Corporativa: Rede de computadores pertencente a uma empresa ou instituição;
V - SI: Segurança da Informação;

VI - SmartCards: Cartão com chip, cujo objetivo é a geração e o armazenamento de certificados digitais;
VII - TI: Tecnologia da Informação;
VIII - Tokens: Pequenos dispositivos que podem ser conectados ao PC para autenticar o usuário, gerando uma senha aleatória.

5. RESPONSABILIDADES:

Responsável	Responsável Atividades
CIINFO	Aprovar e publicar este documento.
Subcomitê de Segurança da Informação e Comunicações	Revisar, monitorar e submeter à aprovação este documento.
Responsáveis descritos de acordo com o item 6 deste documento	Execução de todo o item 6 deste documento.

6. PROCEDIMENTOS:

Regras Gerais de Segurança da Informação para Acesso Remoto

6.1. Disposições Iniciais:

I - O acesso remoto à Rede Corporativa do Ministério da Saúde deve ser realizado somente para atender aos interesses de trabalho do Ministério;
II - O acesso remoto à Rede Corporativa deve ser feito por meio de diferentes perfis de acesso;
III - Compete ao DATASUS definir perfis de acesso, aplicando, quando necessário, técnicas de autenticação e segurança;
IV - Somente os servidores investidos nos cargos de confiança DAS-6, DAS-5, DAS-4 e DAS-3 e nos cargos de natureza especial poderão autorizar o acesso remoto de servidores, atribuindo os respectivos perfis de acesso.

6.2. Quanto ao Controle de Acesso à Rede Corporativa:

I - Os usuários estão sujeitos às técnicas de autenticação que permitam validar a identidade do Usuário da Rede (biometria, tokens, smartcards, entre outros);
II - Compete ao DATASUS a implementação de procedimentos para controlar a concessão e o uso de privilégios especiais de acesso à Rede Corporativa, em

consonância com as definições descritas na Norma de Criação e Manutenção de Contas de Acesso aos Recursos de TI;

III - A área de administração da rede deve realizar uma revisão periódica dos direitos de acesso remoto à Rede Corporativa.

6.3. Quanto ao Acesso Remoto:

I - O acesso remoto, no âmbito da Rede Corporativa, deve ser provido por meio de canal criptografado, preferencialmente utilizando as recomendações da ICP-Brasil;

II - O acesso remoto à Rede Corporativa terá privilégios diferenciados do acesso local, de acordo com o perfil de acesso, com serviços explicitamente controlados;

III - A permissão para se realizar acesso remoto à Rede Corporativa deve ser solicitada à área de administração da rede pela Coordenação ou área superior a que o Usuário da Rede está subordinado, com definição do prazo de validade e horários para se realizar o acesso;

IV - O acesso remoto à Rede Corporativa será gravado, para posterior auditoria, em logs contendo data e hora, serviço utilizado, usuário e informações específicas que facilitem o rastreamento da ação tomada;

V - As permissões de acesso remoto serão revisadas mensalmente.

6.4. Disposições Finais:

I - Os usuários da rede devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à área de gestão de incidentes;

II - Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a área de gestão de incidentes deverá ser imediatamente acionada para tomar as providências necessárias a sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do Ministério da Saúde;

III - Os casos omissos serão resolvidos pelo Subcomitê de Segurança da Informação e Comunicação.

7. DOCUMENTOS COMPLEMENTARES:

Norma de Segurança para Usuário da Rede.

Norma de Criação e Manutenção de Contas de Acesso aos Recursos de TI.

8. ANEXOS:

Não aplicável.

9. CONTROLE DE REGISTROS:

Não aplicável.