# PORTARIA Nº 85, DE 31 DE JANEIRO DE 2012

Legislações - Secretaria Executiva

Qua, 01 de Fevereiro de 2012 00:00

PORTARIA Nº 85, DE 31 DE JANEIRO DE 2012

Publica as normas de Segurança da Informação no âmbito do Ministério da Saúde.

O SECRETÁRIO EXECUTIVO SUBSTITUTO DO MINISTÉRIO DA SAÚDE, no uso de suas atribuições legais, e

Considerando a Instrução Normativa nº 1, de 13 de junho de 2008, do Conselho de Defesa Nacional e da Secretaria-Executiva, que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal;

Considerando a Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações do Ministério da Saúde;

Considerando a Portaria nº 2.072, de 31 de agosto de 2011, que redefine o Comitê de Informação e Informática em Saúde - CIINFO/MS no âmbito do Ministério da Saúde, resolve:

Art. 1º Publicar as normas de segurança da informação dispostas no Anexo a esta Portaria.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

ADRIANO MASSUDA

ANEXO

1 - Normas de Criação e Manutenção de Contas e Acessoaos Recursos de TIC

1) Objetivo:

Esta norma tem por objetivo estabelecer regras para a criação e a administração de contas e acesso aos recursos de Tecnologia da Informação e Comunicações do Ministério da Saúde.

2) Aplicação:

Esta norma aplica-se ao ambiente de trabalho e aos recursos de Tecnologia da Informação do Ministério da Saúde.

3) Documentos de Referência:

I - Norma NBR ISO/IEC 27002 - Código de Práticas para a Gestão da Segurança da Informação;

II - 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;

III - 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;

IV - Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2848/40 - Código Penal, sobre tipificação de crimespor computador contra a Previdência Social e a Administração Pública;

V - Guia de Referência do Ministério do Planejamento para a Rede Governo, que dispõe sobre a formação de contas de usuários. Caixas postais individuais (www.redegoverno.

gov.br/guia_ref/GRNR01.asp) e caixas postais institucionais ( www. redegoverno. gov. br/ guia_ ref/ GRNR02. asp);

VI - Política de Segurança da Informação e Comunicações 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 Segurançada 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 - TI: Tecnologia da Informação;

IV - TIC: Tecnologia da Informação e Comunicações;

V) GP: Gestão de Pessoas;

VI) POSIC/MS: Política de Segurança da Informação e Comunicações do Ministério da Saúde.

5. Responsabilidades:

| Responsável | Atividades |
|---|---|
| CIINFO | Aprovar e publicar este documento. |
| Subcomitê de Segurança da<br><br>Informação e Comunicações | Revisar, monitorar e submeter à aprovação este documento. |
| Demais áreas do Ministério da Saúde | Execução de todo o item 6 deste documento. |

6. Procedimentos:

Regras Gerais para Criação e Manutenção de Contas e Acesso aos Recursos de TIC:

6.1. Disposições Iniciais:

I - Os acessos aos recursos de TIC somente serão permitidos mediante identificação e autenticação dos usuários, mediante conta de acesso;

II - A conta de acesso é pessoal e intransferível, sendo de responsabilidade do usuário

manter a confidencialidade de sua senha pessoal;

III - Ao usuário que não exerce funções de administração da Rede Coorporativa do Ministério da Saúde, deve ser disponibilizada somente uma única conta de acesso, pessoal e intransferível, aos recursos de TIC da Instituição;

IV - O usuário é responsável por todos os acessos realizados por meio da sua conta de acesso à Rede Coorporativa, devendo zelar pelo sigilo da sua conta de acesso e senha, podendo ser responsabilizado pelos possíveis danos que o seu mau uso ocasione aos recursos de TIC da Instituição;

V - O usuário deve evitar a utilização da conta de acesso em mais de uma estação de trabalho ou computador portátil simultaneamente, ficando o Usuário da Rede, titular da conta, responsável pelos riscos da utilização indevida de sua conta de acesso.

6.2. Solicitação de Acessos:

I - Os direitos de acesso devem ser solicitados de acordo com as necessidades do setor para a execução das suas atividades;

II - Para servidores públicos em exercício no Ministério, a criação de contas de acesso será realizada pela Coordenação-Geral de Gestão de Pessoas quando da "investidura" do servidor no Ministério da Saúde, estando condicionada à assinatura do Termo de Responsabilidade pelo usuário;

III - Para os demais agentes públicos, a criação de contas de acesso somente será realizada mediante solicitação formal, com a devida justificativa à área de Gestão de Pessoas pelo chefe imediato do agente público ou seu superior formalmente investido no cargo, e desde que o usuário esteja devidamente cadastrado no Sistema Integrado de Administração de Recursos Humanos - SIARH e assine o Termo de Responsabilidade;

IV - Quando houver mudança nas atribuições de um Usuário da Rede ou quando ocorrer o seu remanejamento para outro setor, os direitos de acesso deverão ser readequados, por solicitação dos superiores imediatos;

V - Os visitantes do Ministério da Saúde podem solicitar acesso exclusivamente à Internet, que se dará por tempo determinado e de acordo com procedimentos definidos pelo DATASUS.

6.3. Criação e Manutenção de Contas de Acesso:

I - O nome de usuário seguirá a nomenclatura padronizada pelas Regras de formação de nomes para a composição de endereço eletrônico (e-mail) no Governo Federal, publicadas pelo Ministério do Planejamento e já em uso pelo Ministério da Saúde, disponíveis em: https:// www. governoeletronico. gov. br/ biblioteca/ arquivos/ regras- deformacao- de-nomes-para-a-composicao-de-endereco-eletronico-email- no-governo-federal/download;

II - Na formação de nomes, deve ser utilizada a forma mais simples de composição, qual seja um nome seguido de ponto e de um sobrenome, devendo ser priorizado o uso de nomes pelos quais o usuário é publicamente conhecido;

III - Na liberação da conta de acesso do Usuário da Rede, será fornecida uma senha temporária, a ser alterada obrigatoriamente no seu primeiro acesso;

IV - A senha de acesso aos recursos de TI deve ser obrigatoriamente alterada a cada 90 (noventa) dias ou sempre que o Usuário da Rede desejar;

V - O Usuário da Rede será notificado da expiração da senha com 8 (oito) dias de

antecedência;

VI) A senha deve ser composta obrigatoriamente por, no mínimo, 8 (oito) caracteres, sendo, pelo menos, 4 (quatro) deles numéricos ou especiais e os demais, alfabéticos;

VII) Deve-se evitar a utilização de informações pessoais na criação da senha de acesso à Rede Local;

VIII) O Usuário da Rede não poderá reutilizar as últimas 4 (quatro) senhas registradas nem repeti-las no prazo de 30 dias. 6.4. Bloqueio da Conta de Acesso:

I - A conta de acesso será bloqueada nas seguintes situações:

a) Após 5 (cinco) tentativas de acesso mal sucedidas;

b) Sem utilização há mais de 60 (sessenta) dias, quando o bloqueio deverá ser informado à chefia imediata ou superior do Usuário da Rede.

II - O desbloqueio da conta de acesso deverá ser solicitado ao Serviço de Suporte ao Usuário.

6.5. Suspensão da Conta de Acesso:

I - Ocorrerá quando solicitada pela chefia imediata ou superior do Usuário da Rede, devendo ser formalmente justificada;

II - Sempre que houver suspeita de que a utilização do serviço esteja infringindo a POSIC/MS, esta norma ou normas correlatas em vigor, o serviço será temporariamente suspenso pelo DATASUS até que se complete a apuração dos fatos;

III - Por solicitação da área de RH, quando do afastamento do Usuário da Rede em decorrência de Processo Administrativo Disciplinar, cessão do funcionário a outro órgão ou outros afastamentos que o justifiquem;

IV - A reativação da conta de acesso deve ser realizada mediante solicitação formal da chefia imediata ou superior do Usuário da Rede à área de Gestão de Pessoas, que deverá informar ao DATASUS.

6.6. Cancelamento da Conta de Acesso:

I - As contas de acesso não utilizadas, sem justificativa, por mais de 120 dias serão automaticamente canceladas e o cancelamento notificado à chefia imediata ou superior do Usuário da Rede;

II - Para servidores efetivos, quando do desligamento do Ministério da Saúde, o cancelamento da sua conta de acesso deverá ser imediatamente efetuado pela área de Gestão de Pessoas, que deverá informar ao DATASUS;

III - Para demais usuários, quando do seu desligamento ou interrupção do vínculo com o Ministério da Saúde, o cancelamento da sua conta de acesso deverá ser formalmente solicitado pelo chefe imediato ou superior à área de Gestão de Pessoas, que deverá informar

ao DATASUS.

6.7. Disposições Transitórias:

I - Os Usuários da Rede já cadastrados e que possuem acesso aos recursos de TI devem, no prazo máximo de 60 dias a contar da publicação desta norma, dar ciência do Termo de

Responsabilidade e com ele concordar, para terem acesso à Rede Coorporativa do MS;

II - Passados 60 dias, os Usuários que não aderirem ao Termo de Responsabilidade terão seus acessos suspensos;

III - Os Usuários da Rede já cadastrados e em desacordo com a nomenclatura padronizada, conforme determinado pelo subitem I do item 6.3, terão o nome de usuário ajustado, segundo procedimento estabelecido pelo DATASUS.

6.8. 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 caso de quebra de segurança da informação por meio de recursos de TI, a área de gestão de incidentes deverá ser imediatamente acionada, para tomar as providências necessárias a sanar as causas do problema, podendo, inclusive, determinar a suspensão temporária do acesso às informações e/ou do uso dos recursos de TI do Ministério da Saúde;

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

7. Documentos Complementares:

Guia de Referência do Ministério do Planejamento para a Rede Governo.

8. Anexos:

Termo de Responsabilidade.

9. Controle de Registros:

Não aplicável.

2 - Normas de Segurança para o Uso do Correio Eletrônico

1. Objetivo:

Orientar os Usuários da Rede do Ministério da Saúde quanto às regras de utilização do serviço de correio eletrônico de forma a preservar a confidencialidade, a integridade e a disponibilidade das informações.

2. Aplicação:

Esta norma de segurança aplica-se ao ambiente de trabalho e aos recursos de tecnologia da informação do Ministério da Saúde.

3. Documentos de Referência:

I - Norma NBR ISO/IEC 27002 - Código de Práticas para a Gestão da Segurança da Informação;

II - ISO/IEC Guide 73.2002 - Gestão de Riscos / Vocabulário - Recomendações para uso em normas;

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 e Comunicação do Ministério da Saúde;

VI - Cartilha de segurança para a Internet, versão 3.1 do cert.br - http://cartilha.cert.br/.

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 - Correio Eletrônico: É um sistema que permite a troca de mensagens entre usuários. Cada usuário deste sistema possui um endereço eletrônico e uma caixa postal própria;

IV - Caixa postal individual: Caixa postal de correio eletrônico para uso individual associada a um único usuário da rede;

V - Caixa postal institucional - Caixa postal de correio eletrônico associada a uma unidade organizacional do Ministério da Saúde. Essa associação será feita, preferencialmente, adotando-se a sigla da unidade para a composição do endereço de correio eletrônico;

VI - POSIC/MS - Política de Segurança da Informação e Comunicação do Ministério da Saúde.

5. Responsabilidades:

| Responsável | Atribuição |
|---|---|
| CIINFO | Aprovar e publicar este docu- mento. |
| Subcomitê de Segurança da Infor- mação do Ministério da Saúde | Revisar, monitorar e encami- nhar este documento para apro- vação. |
| Responsáveis descritos de acordo com o item 6 deste documento | Execução de todo o item 6 des- te documento. |

6. Procedimentos:

Regras Gerais de Segurança da Informação para Correio Eletrônico

6.1. Disposições Iniciais:

I - A conta de correio eletrônico corporativo, disponibilizado aos Usuários da Rede pelo Ministério da Saúde, deve ser utilizada somente para os interesses de trabalho do Ministério

da Saúde;

II - A conta de correio eletrônico terá a mesma identificação da conta de acesso aos recursos de TI;

III - A conta de correio eletrônico corporativo disponibilizado ao Usuário da Rede do Ministério da Saúde é pessoal e intransferível, sendo seu titular o único e total responsável pelo seu uso e suas consequências;

IV - É atribuição exclusiva do DATASUS definir os softwares homologados para o uso do correio eletrônico corporativo e da Internet, incluindo serviços de mensagens instantâneas, voz, videoconferência e de transferência de arquivos;

V - O Ministério da Saúde permite o uso parcimonioso do correio eletrônico particular para interesses particulares dos Usuários da Rede, desde que esse uso não exceda os limites da ética, bom senso e razoabilidade;

6.2. Permissão de acesso e criação de contas:

I - Os superiores imediatos dos Usuários da Rede do Ministério da Saúde devem avaliar a necessidade de utilização do correio eletrônico corporativo para os seus subordinados, indicando tal necessidade quando da solicitação da criação da conta de acesso aos recursos de TI;

II - A vigência da conta de correio eletrônico corporativa deve seguir as orientações contidas na Norma de Criação e Manutenção de Contas de Acesso aos Recursos de TI;

III - Para cada Usuário da Rede do Ministério da Saúde, é concedida apenas uma única conta de correio eletrônico individual, vinculada à sua conta de acesso aos recursos de TI, conforme definições descritas na "Norma de criação e manutenção de contas de acesso aos Recursos de TI";

IV - A criação de correio eletrônico corporativo institucional deve ser solicitada ao DATASUS somente pelo gestor departamental, justificando formalmente sua utilização;

V - O correio eletrônico corporativo institucional pode ser acessado por vários Usuários da Rede simultaneamente, mas deve ter apenas um responsável e um substituto, os quais deverão ser indicados pelo gestor departamental solicitante, ficando este vinculado à conta de acesso do gestor.

6.3. Cancelamento, bloqueio, suspensão ou desbloqueio do correio eletrônico:

I - A utilização do correio eletrônico corporativo é uma concessão do Ministério da Saúde, que será cancelada quando de desligamento, ao final da vigência do contrato, devido a qualquer outro ato jurídico firmado ou por solicitação do superior imediato;

II - No caso de desligamento definitivo do usuário, este poderá, facultativamente, configurar uma resposta automática de desligamento, por um período de 180 dias;

III - Nos casos de afastamento temporário do servidor público, o acesso à sua caixa de correio eletrônico poderá permanecer ativo mediante solicitação à área de RH;

IV - Nos casos de suspensão do servidor público, o acesso à caixa de correio eletrônico também será suspenso e somente será liberado pelo departamento de RH;

V - O cancelamento, o bloqueio, a suspensão e o desbloqueio da conta de correio eletrônico corporativo seguem as condições descritas na Norma de criação e manutenção de contas de

acesso aos Recursos de TI;

6.4. Uso do correio eletrônico:

I - As caixas postais do correio eletrônico corporativo possuem capacidade limitada de espaço, conforme a capacidade e disponibilidade de área de armazenamento, ficando a cargo do DATASUS definir os limites de capacidade das caixas de correio eletrônico;

II - Os arquivos a serem anexados às mensagens no correio eletrônico corporativo não poderão ultrapassar o limite de tamanho, conforme estabelecido pelo Datasus;

III - É vedado o envio de mensagens eletrônicas para mais de 100 destinatários em uma mesma mensagem, devendo-se, para esses casos, utilizar o serviço de listas de destinatários para envio de mensagens.

IV - É vedada a utilização do correio eletrônico corporativo para:

a) Realizar SPAM;

b) Contribuir com a continuidade de correntes de mensagens eletrônicas;

c) Objetivos político-partidários;

d) Receber de forma consentida, armazenar ou enviar mensagens com vírus de computador, cavalo-de-tróia, spyware e outros códigos maliciosos, bem como contendo material pornográfico, atentatório à moral, ofensivo, com conteúdo ilegal, criminoso ou que faça apologia ao crime, de incitação à violência ou com conteúdo que não respeite os direitos autorais.

V - De forma a preservar o funcionamento do serviço de correio eletrônico corporativo, o Usuário da Rede deve:

a) Eliminar, periodicamente, as mensagens desnecessárias de sua caixa postal, inclusive as existentes nas pastas personalizadas, na lixeira, em rascunho e as enviadas, de forma a não exceder o limite de tamanho da caixa postal;

b) Evitar clicar em links de acesso a páginas de Internet existentes em mensagens de correio eletrônico recebidas de origem desconhecida, pois esses podem iniciar a instalação de softwares maliciosos ou direcionar o Usuário da Rede para um sítio falso, possibilitando a captura de informações;

c) Evitar abrir ou executar arquivos anexados às mensagens recebidas pelo correio eletrônico sem antes verificá-los quanto à possibilidade de contaminação por vírus de computador. Nos casos da existência de arquivos contaminados, o Usuário da Rede, quando não solucionar o problema, deve solicitar ajuda ao DATASUS;

d) Compactar grandes arquivos a serem anexados nas mensagens do correio eletrônico corporativo, mediante utilização do software de compactação homologado e disponibilizado na estação de trabalho.

VI - Todo Usuário da Rede do Ministério da Saúde, antes de enviar mensagens pelo correio eletrônico corporativo, deve: a) Levar em conta o sigilo da informação a ser encaminhada, cabendo a ele consultar o Gestor de Informação se tiver dúvidas, assim como providenciar a adequada forma de envio, consultando o DATASUS quanto aos meios de transmissão segura;

b) Respeitar os direitos autorais de terceiros no conteúdo de suas mensagens.

VII - O uso da conta de correio eletrônico corporativo em listas de discussão ou distribuição

deve limitar-se aos casos de necessidade do trabalho ou atividade desempenhada no Ministério da Saúde;

VIII - O correio eletrônico particular deverá ser usado somente para interesses particulares do Usuário da Rede, não podendo ser utilizado para o envio ou recebimento de informações do Ministério da Saúde;

IX - O acesso ao correio eletrônico particular utilizando-se de estação de trabalho ou equipamento eletrônico portátil do Ministério da Saúde somente será permitido via browser;

X - O Ministério da Saúde não se responsabiliza pelas mensagens de correio eletrônico particular armazenadas em seus equipamentos ou pelo suporte a estes serviços de correio.

6.5. Monitoramento:

I - O correio eletrônico corporativo pode ser monitorado e restringido pelo DATASUS quanto à origem, destino, quantidade, tipo de conteúdo, tipo de anexo e volume das informações, desde que esses controles sejam feitos por parâmetros gerais (não personalizados);

II - Nos casos de suspeita de infração à Política de Segurança da Informação em vigor e a normas correlatas, o DATASUS pode acessar a caixa postal corporativa do Usuário da Rede em questão;

III - O acesso à caixa postal corporativa de outro usuário somente será concedido mediante autorização formal ou em virtude de ato administrativo ou judicial.

6.6. Disposições Finais:

I - Toda mensagem enviada pelo serviço de correio eletrônico do Ministério da Saúde conterá o texto de "Aviso Legal" a seguir, em português e em inglês, inserido automaticamente pelo serviço de mensageria, sem prejuízo de outras mensagens do próprio usuário:

"Esta mensagem pode conter informação confidencial e/ou privilegiada. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não pode usar, copiar ou divulgar as informações nela contidas ou tomar qualquer ação baseada nessas informações.

Se você recebeu esta mensagem por engano, por favor avise imediatamente o remetente, respondendo o e-mail e em seguida apague-o.

This message may contain confidential and / or privileged. If you're not the recipient or the person authorized to receive this message, you can not use, copy or disclose the information contained therein or take any action based on this information. If you have received this message in error, please notify the sender immediately by reply e-mail and then delete it."

II - Compete à Assessoria de Comunicações - ASCOM qualquer alteração do texto de "Aviso Legal".

7. Documentos Complementares:

Norma de Criação e Manutenção de Contas e Senhas.

8. Anexos:

Não aplicável.

9. Controle de Registros:

Não aplicável.

3 - 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.

V - SmartCards: Cartão com chip, cujo objetivo é a geração e o armazenamento de certificados digitais.

VI - TI: Tecnologia da Informação.

VII - Tokens: Pequenos dispositivos que podem ser conectados ao PC para autenticar o

usuário, gerando uma senha aleatória.

5) Responsabilidades:

| Responsável | Atividades |
|---|---|
| CIINFO | Aprovar e publicar este documen- to. |
| Subcomitê de Segurança da In- formação e Comunicações | Revisar, monitorar e submeter à aprovação este documento. |
| Responsáveis descritos de acor- do com o item 6 deste docu- mento | 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 deacesso 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 utilizandoas 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.

4 - Normas de Segurança para Uso de Internet

1) Objetivo:

Esta norma tem como objetivo informar aos usuários da rede do Ministério da Saúde quanto às regras de utilização do serviço de Internet, de forma a preservar a confidencialidade, a integridade e a disponibilidade das informações.

2) Aplicação:

Esta norma se aplica ao Ministério da Saúde.

3) Documentos de Referência:

I - NBR ISO/IEC 17799:2005 - Código de Práticas para a Gestão de Segurança da Informação;

II - ISO/IEC Guide 73:2002 - Gestão de Riscos/Vocabulário - Recomendações para uso em normas;

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;

VI - Cartilha de segurança para a Internet, versão 3.1 do cert.br - http://cartilha.cert.br.

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.

5) Responsabilidades:

| Responsável | Atribuição |
|---|---|
| CIINFO | Aprovar e publicar este docu- |
| Subcomitê de Segurança da Infor- mação e Comunicações do Minis- tério da Saúde | Revisar<br><br>nhar este documento para apro- vação. |
| Responsáveis descritos de acordo com o item 6 deste documento | Execução de todo o item 6 deste documento. |

6) Procedimentos:

Regras Gerais para Uso da Internet

6.1. Disposições Iniciais:

I - O acesso à Internet disponibilizado pelo Ministério da Saúde aos usuários da rede deve ser utilizado para os interesses de trabalho da Instituição;

II - O Ministério da Saúde permite o uso da Internet para fins particulares dos Usuários da Rede, desde que este uso não exceda os limites da ética, do bom senso e da razoabilidade;

III - É atribuição exclusiva do DATASUS definir os softwares homologados para o uso da Internet no Ministério da Saúde;

IV - O acesso à Internet não pode ser realizado utilizando-se mais de um canal (link) de comunicação simultaneamente em uma mesma estação de trabalho.

6.2. Permissão de Acesso à Internet:

I - A todo usuário da rede local do MS, é facultado o acesso à Internet, em conformidade com os termos estabelecidos nesta norma.

6.3. Cancelamento e Bloqueio do Acesso à Internet:

I - O acesso à Internet pelo Usuário da Rede será obrigatoriamente cancelado quando do desligamento, ao final do contrato ou decorrente de qualquer outro ato jurídico que mantém vínculo com a Instituição;

II - O cancelamento, o bloqueio e o desbloqueio do acesso à Internet seguem as condições descritas na Norma de Criação e Manutenção de Contas e Senhas.

6.4. Uso da Internet:

I - O acesso à Internet concedido ao Usuário da Rede do Ministério da Saúde é pessoal e intransferível, sendo seu titular o único e total responsável pelas ações e danos causados à Instituição por meio de seu uso;

II - O acesso à Internet, quando realizado pela Rede Local disponibilizada pelo DATASUS e por meio do browser homologado e disponibilizado nas estações de trabalho do Ministério da Saúde ou equipamentos portáteis, não poderá ser feito mediante proxies externos, que permitem burlar as regras de acesso estabelecidas;

III - O Usuário da Rede deverá utilizar a Internet de forma a não causar tráfego desnecessário na Rede Local do Ministério da Saúde ou em redes de outras instituições;

IV - Todo serviço disponibilizado na Internet, antes de ser disponibilizado na rede local do Ministério da Saúde, deverá ser avaliado quanto à sua necessidade pelo Subcomitê de Segurança da Informação, após a avaliação e a emissão de relatório técnico fornecido pelo DATASUS, que deverá considerar os aspectos de segurança da informação, o consumo de recursos tecnológicos e o comprometimento de outros serviços;

V - O DATASUS deverá publicar na Intranet, de forma consolidada, relatórios que demonstrem o uso da Internet no ambiente do Ministério da Saúde, ficando vedada a divulgação de dados de acesso individualizados. Esses dados poderão ser fornecidos à coordenação ou ao setor hierarquicamente superior responsável pelo usuário, mediante solicitação formal, ou, nos caso de desvios no uso da Internet, ser informados ao Subcomitê de Segurança da Informação e Comunicação;

VI - É vedada a utilização da Internet para:

a) Acessar sítios com códigos maliciosos e vírus de computador;

b) Acessar sítios com materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;

c) Acessar sítios ou arquivos com conteúdo ilegal, criminoso ou que façam apologia ao crime, incluindo os de pirataria ou que divulguem número de série para registro de softwares;

d) Acessar sítios ou arquivos com conteúdo de incitação à violência;

e) Realizar download de arquivos que não estejam relacionados às necessidades de trabalho do Ministério da Saúde, em especial arquivos que contenham materiais ilegais ou que não

respeitem os direitos autorais;

f) Realizar atividades relacionadas a jogos eletrônicos pela Internet;

g) Escutar música ou assistir programas de TV, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho do Ministério da Saúde; e

h) Transferir e armazenar informações sensíveis do Ministério em sites com os quais não haja um contrato ou acordo de responsabilidade estabelecido com esta Instituição.

VII - É de responsabilidade do DATASUS garantir os serviços de transferência e compartilhamento de arquivos com informações do Ministério da Saúde na Internet de forma segura;

VIII - O usuário sempre deverá certificar a procedência do sítio, verificando, quando cabível, seu certificado digital, principalmente para realizar transações eletrônicas via Internet, digitando o endereço do sítio diretamente no browser da estação de trabalho, nunca clicando em um link existente em uma página ou em uma mensagem de correio eletrônico;

IX - O DATASUS deverá homologar softwares ou serviços de mensagens instantâneas, de voz, de videoconferência e de transferência de arquivos via Internet;

X - É vedado aos usuários disponibilizar informações de propriedade do Ministério da Saúde em sites da Internet sem observar sua classificação e o público a que se destina;

XI - Só será permitida a utilização da rede local por máquinas que atendam a todos os requisitos de segurança da informação estabelecidos pelo DATASUS;

XII - A conexão de equipamentos pessoais à rede do Ministério da Saúde poderá ser autorizada exclusivamente para acesso à Internet;

XIII - Fica liberado o acesso a sítios de governo, de órgãos de ensino e pesquisa, de organismos internacionais, de pesquisa, de órgãos técnico-normativos e a jornais e revistas de cunho cultural e educativo, bem como a outros de interesse institucional.

6.5. Monitoramento:

I - O acesso à Internet deve ser monitorado, podendo ser divulgado e restringido pelo DATASUS quanto a endereço, quantidade, horário, tempo de permanência, tipo de conteúdo e volume de informações trafegadas, desde que esses controles sejam feitos por parâmetros gerais (não personalizados);

II - O superior imediato pode solicitar formalmente um relatório com as informações de acesso à Internet de um de seus Usuários da Rede, para si ou para outro, nas seguintes situações:

a) Suspeita de infração à Política de Segurança da Informação em vigor e normas correlatas;

b) Necessidade de visualizar os sites acessados e o tempo neles gasto por seus Usuários de Rede.

6.6. 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 fim de 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 usuários da Rede que descumprirem as regras estabelecidas por esta Norma poderão ter seu acesso à rede bloqueado até a apuração de responsabilidades;

IV - O DATASUS poderá adotar, a qualquer momento, medidas excepcionais que sejam necessárias para garantir a segurança, a disponibilidade, a integridade, a confidencialidade e a estabilidade da rede;

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

7. Documentos Complementares:

Norma de Criação e Manutenção de Contas de Acesso aos Recursos de TIC

8. Anexos:

Não aplicável.

9. Controle de Registros:

Não aplicável.