Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul

Regulamento

Política da Segurança da Informação

INSTITUTO FEDERAL
MATO GROSSO DO SUL

Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul

Regulamento
Política da Segurança da Informação

IFMS | 2011

Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul

Regulamento nº 002 Política da Segurança da Informação | IFMS

Instituto Federal de Educação,
Ciência e Tecnologia de Mato Grosso do Sul - IFMS

Marcus Aurélius Stier Serpe
Reitor

Assessoria de Tecnologia da Informação
Wilian Dias
Reitoria - Publicação 020/ 2011

ASCOM - IFMS
Wilmara Rios | Programação Visual
Isabella Saliba Pereira | Revisão gramatical

Setembro 2011
Campo Grande | MS

Regulamento
Política da Segurança da Informação

IFMS | 2011

Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul

INSTITUTO FEDERAL
MATO GROSSO DO SUL

Sumário

Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul

REGULAMENTO Nº 002, DE 7 DE FEVEREIRO DE 2011.

Dispõe acerca da Política de Segurança da Informação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul (IFMS).

O REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO DO SUL, no uso de suas atribuições legais, conferidas pela Portaria Ministerial nº 39 de 7 de janeiro de 2009, publicada no D.O.U. de 8 de janeiro de 2009;

Considerando a necessidade de normatizar a criação de contas para correio eletrônico institucional;

RESOLVE:

Art. 1º - Dispor sobre a política de disponibilização e utilização dos recursos de tecnologia da informação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul.

Capítulo I
DOS OBJETIVOS

Art. 2° - Estabelecer regras para a disponibilização e utilização de serviços de rede de dados, internet, telecomunicações e correio eletrônico institucional.

Art. 3° - Aprovar as políticas, normas e procedimentos de segurança da informação;

Art. 4º - Designar, definir ou alterar as responsabilidades da área de Segurança da Informação;

Art. 5º - Aprovar novos controles ou alterar as responsabilidades da área de Segurança da Informação;

Art. 6º - Apoiar a implantação de soluções para a minimização dos riscos;

Art. 7º - Dar suporte às iniciativas na área de Segurança da Informação;

Art. 8º - Priorizar soluções, programas e serviços baseados em *software* livre que promovam a otimização de recursos e investimentos em tecnologia da informação em todos os níveis institucionais.

Capítulo II

DAS CONSIDERAÇÕES GERAIS

Art. 9° - Este instrumento é projetado para assegurar que todos os usuários que utilizam diretamente ou indiretamente recursos computacionais, serviços de internet, rede de dados, telefonia e correio eletrônico providos pelo Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul possam fazer uso consciente e responsável dos mesmos.

Art. 10 - O IFMS poderá utilizar ferramentas, técnicas e tecnologias que permitirão o monitoramento, controle e armazenamento de registros de acesso e conteúdo de quaisquer formas de comunicação que se utilizem da infraestrutura provida pelo Instituto.

Art. 11 - A utilização dos recursos de rede de dados, internet, telecomunicações, correio eletrônico e recursos computacionais devem estar em conformidade com a missão do Instituto e respeitar a finalidade acadêmica ou laboral dos recursos do IFMS.

Art. 12 - Todo acesso à rede local, internet, intranet e extranet deverá ser feita através de um *login* de acesso único, pessoal e intransferível.

Capítulo III

DAS RESPONSABILIDADES E PROIBIÇÕES

Art. 13 - A responsabilidade pela segurança das informações deverá estar estabelecida nos documentos oficiais do IFMS e principalmente na Política de Segurança da Informação.

Art. 14 - Cada servidor público é responsável pela Segurança das informações dentro do IFMS, principalmente pelas informações que estão sob sua responsabilidade.

Art. 15 - O monitoramento do uso da internet é importante para que sejam registrados todos os acessos de cada usuário e para que possam ser notificados e até mesmo punidos nos casos de acesso que sejam contrários a política do IFMS.

Art. 16 - Para fins de auditoria e comprovação dos acessos é indispensável que algumas informações sejam armazenadas juntamente com os sites utilizados. Alguns dos principais dados que precisam ser armazenados são: identidade do usuário, data e hora da conexão, endereço IP de origem, protocolos utilizados e quantidade de dados sendo transmitidos e/ ou recebidos, além dos LOGs dos servidores que devem ser mantidos por um período mínimo de 24 meses.

Art. 17 – São responsabilidades dos usuários de serviços de rede de dados, internet, telecomunicações e correio eletrônico e recursos computacionais do Instituto Federal de Mato Grosso do Sul:

Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de suas respectivas senhas;

Seguir de forma colaborativa as orientações fornecidas pelos setores competentes em relação ao melhor uso dos recursos computacionais, de rede de dados, internet, telecomunicações e correio;

Efetuar cópias de segurança de seus arquivos, catálogos de endereço, e-mails e quaisquer outros materiais de ordem digital;

Utilizar de forma ética e legal os recursos computacionais, de rede de dados, internet, telecomunicações e correio eletrônico;

Não alterar configurações dos softwares de segurança como antivírus e *firewall*.

Art. 18 – São proibições aos usuários de serviços de rede de dados, internet, telecomunicações e correio eletrônico e recursos computacionais do Instituto Federal de Mato Grosso do Sul:

Utilizar, em quaisquer circunstâncias, os recursos do Instituto Federal de Mato Grosso do Sul para difamar, prejudicar, subtrair, caluniar ou molestar outras pessoas ou Instituições;

Utilizar, examinar, copiar, armazenar, distribuir ou instalar programas ou qualquer material protegido por direito autoral (*copyright*);

Utilizar, em quaisquer circunstâncias, os recursos do Instituto Federal de Mato Grosso do Sul em campanhas políticas e/ou propagandas comerciais;

Efetuar qualquer tipo de acesso e/ou alteração em dados não autorizados;

Violar ou tentar violar sistemas de segurança do Instituto Federal de Mato Grosso do Sul ou de qualquer outra Instituição ou pessoa;

Fazer-se passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos da Instituição;

Transmitir, difundir ou disponibilizar a terceiros, informações, dados, conteúdos, mensagens, gráficos, desenhos, arquivos e som e/ou imagem, fotografias, gravações, software ou qualquer classe de material que, de qualquer formam, induzam, incitem ou promovam atos ilegais, denegridores, difamatórios, infames, violentos ou, em geral, contrários à lei, à moral e aos bons costumes geralmente aceitos ou à ordem pública;

Capítulo IV
DAS SENHAS

Art. 19 - As senhas de acesso não devem ser compartilhadas ou divulgadas, evitando-se, assim, que outros usuários não permitidos tenham acesso a informações confidenciais ou que não lhes digam respeito.

Art. 20 – Por serem de fácil dedução, alguns critérios devem ser evitados na criação de uma senha:

números sequenciais;

datas de nascimento;

sobrenome;

placas de carros, entre outros.

Art. 21 - Os sistemas devem ser configurados de forma a não permitir a criação de senhas consideradas de fácil descobrimento, contendo parâmetros básicos como:

Número de caracteres para composição da senha: no mínimo seis caracteres;

Expiração de senha: deve ser forçada a alteração das senhas dos usuários no período de 6 meses;

Repetição de senhas: restringir, pelo menos, a utilização das ultimas cinco senhas utilizadas;

Quantidade de tentativas inválidas de acesso: deve haver um limite de três tentativas para realizar o bloqueio de acesso inválido, de forma a evitar a descoberta das senhas;

Troca de senhas iniciais (*default*): As senhas iniciais dos sistemas, banco de dados e quaisquer outros serviços devem ser trocados de forma imediata, antes de sua utilização em ambiente seguro;

Bloqueio automático por tempo de inatividade (*Time out*): Os sistemas devem possuir tempo máximo determinado para realizar bloqueio/término de um acesso por inatividade.

Capítulo V
DAS ESTAÇÕES DE TRABALHO

Art. 22 - As estações devem ser empregadas apenas para a realização de atividades que estão diretamente relacionadas ao trabalho do servidor e às normas do IFMS, considerando os seguintes parâmetros:

Monitoramento para que usuários não instalem *softwares* que não são homologados pelo IFMS e que, consequentemente, não possuem licença de uso;

Bloqueio de quaisquer tipos de jogos ou outros aplicativos que possam reduzir o desempenho dos usuários;

Padronização das permissões de acordo com o que cada departamento ou servidor público necessita, restringindo o acesso a outros dados que não digam respeito àquele departamento;

Dispositivo de bloqueio das estações de trabalho, mediante senha, quando os usuários ausentarem-se de seu local de trabalho, a fim de coibir que usuários não autorizados tenham acesso. Podendo ser utilizada a própria proteção do sistema operacional, proteção de tela com senha ou qualquer recurso oferecido para esta finalidade;

Controles sobre os dispositivos de I/O (entrada e saída) e de informações no IFMS, como: drives de disquete, gravadores de CDs, gravadores de DVDs, dispositivos USBs e quaisquer outros meios físicos que permitam a entrada e principalmente a saída de informações sem controle. A saída ou utilização destes recursos deve ser autorizada formalmente;

Dispositivos extras de segurança que bloqueiem o acesso não autorizado às informações contidas nas estações de trabalho móveis (*laptops*);

Acesso restrito aos recursos de internet;

Art. 23 - As estações de trabalho deverão ter, por padrão, seu disco rígido dividido em duas partições: uma para o sistema e outra para dados.

Capítulo VI
DAS REALIZAÇÕES DE *BACKUPS*

Art. 24 – Deverão ser adotados, independentemente de seu tamanho, procedimentos de cópias de segurança (*backup*) e recuperação (*restore*) de informações.

Art. 25 - Para a implementação da cópia de segurança deve-se levar em consideração a importância da informação, o nível de classificação utilizado, sua periodicidade de atualização e também sua volatilidade, conforme as seguintes premissas:

Realizar *backup* visando diminuir os riscos de continuidade;

Manter os *backups* em local físico distante da localidade de armazenamento dos dados originais;

Verificar a integridade da informação armazenada;

Avaliar a funcionalidade dos procedimentos;

Identificar procedimentos desatualizados ou ineficazes;

Identificar falhas ou defeitos.

Art. 26 – São de responsabilidade do departamento de Tecnologia da Informação do IFMS os procedimentos relacionados à política de *backups* de dados:

Documentar, testar e avaliar regularmente as tarefas de *backup*;
Aplicar testes de recuperação e validação dos *backups* mensalmente;
Alocar o servidor de backup em local seguro e isolado, visando à segurança, integridade e inviolabilidade dos dados;

Art. 27 - A política de *backups,* de acordo com o serviço, deverá ocorrer da seguinte maneira:
Diário, e de preferência Incremental, nos servidores de bancos de dados do IFMS. Esses *backups* devem ser automáticos e preferencialmente em períodos em que não haja atividade intensa na rede;
Semanal do conteúdo dos servidores WWW, DNS, LDAP, PDC Samba, Proxy, Firewall e VPN, se houver.

Art. 28 – Antes do descarte de discos ou outros equipamentos deverá ser assegurado de que as informações importantes foram salvas em cópias de segurança e de que tais equipamentos serão definitivamente destruídos, sem risco de comprometer a confidencialidade das informações do IFMS.

Capítulo VII

DO GERENCIAMENTO, CONTROLE DA REDE, MONITORAÇÃO DO USO E ACESSO AOS SISTEMAS

Art. 29 - Os controles de acesso lógico devem assegurar que:

Apenas os usuários autorizados tenham acesso aos recursos;

Os usuários tenham acesso apenas aos recursos realmente necessários para a execução de suas atividades.

O acesso aos recursos críticos seja constantemente monitorado e restrito;

Os usuários sejam impedidos de executar transações incompatíveis com a sua função.

Art. 30 - Controle de acesso pode ser resumido nas funções:

Identificação e autenticação de usuários;

Gerenciamento e monitoramento de privilégios;

Limitação e desabilitação de acessos e prevenção de acessos não autorizados.

Art. 31 – Deverão ser organizadas revisões periódicas das contas de usuários e de seus respectivos privilégios. A organização deve padronizar os seguintes aspectos:

Todas as solicitações de acesso devem ser formais e devidamente aprovadas pelos níveis requeridos;

Revisões periódicas sempre que houver alguma alteração no ambiente dos sistemas, incluindo também administradores ou quaisquer outros tipos de acesso privilegiado;

As contas dos usuários afastados ou em férias devem ser bloqueadas temporariamente;

A comunicação dessas situações deve ocorrer por meio de procedimento efetuado pelo departamento de pessoal ou de recursos humanos. A periodicidade da comunicação deve ser mensal para os casos de afastamento e férias.

CapítuloVIII

DO DESCUMPRIMENTO DAS REGRAS E PENALIDADES

Art. 32 - O descumprimento ou inobservância de quaisquer regras ou políticas definidas neste instrumento ou em outros a serem implementados pelo IFMS são consideradas faltas graves, podendo, sem prejuízo das ações disciplinares previstas no Regime Juridico Único e no Estatuto do Instituto, resultar na instauração, contra o infrator, de ações extrajudiciais cíveis e criminais, além da suspensão imediata dos privilégios de acesso e uso dos recursos computacionais do Instituto.

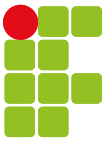
Art. 33 – Este Regulamento entra em vigor na data de sua publicação no site do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul.

Campo Grande, MS, 7 de fevereiro de 2011.

Marcus Aurélius Stier Serpe

Reitor

MINISTÉRIO DA EDUCAÇÃO



INSTITUTO FEDERAL
MATO GROSSO DO SUL

Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul | IFMS
Reitoria: Rua Ceará, 972
Bairro Santa Fé | Campo Grande | MS | CEP: 79021-000
(67) 3042.5117 | www.ifms.edu.br