GOVERNO DO ESTADO DE MINAS GERAIS

[Instituto de Previdência dos Servidores Militares do Estado de Minas Gerais]

[Assessoria de Tecnologia da Informação]

PORTARIA DG Nº 1124/2023

Institui a Política de Segurança da Informação - PSI , no âmbito do Instituto de Previdência dos Servidores Militares - IPSM.

O Diretor-Geral do Instituto de Previdência dos Servidores Militares do Estado de Minas Gerais (IPSM), no uso das atribuições que lhe confere art. 7º, inciso I, do Decreto 48.064, de 16 de outubro de 2020, RESOLVE:

Art. 1º - Instituir a **Política de Segurança da Informação - PSI** no âmbito do IPSM, conforme normas nesta Portaria.

Art. 2º - **DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI-001**

I - **O IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DE MINAS GERAIS** tem como missão, garantir o benefício previdenciário e promover a atenção à saúde por meio de ações administrativas, em prol da segurança e qualidade de vida da Família Militar Mineira. Tem como visão, ser reconhecido como Entidade de excelência na gestão do Regime Próprio de Previdência dos militares do Estado e na promoção da assistência à saúde. Tem como princípios e valores da Confidencialidade, Integridade, Disponibilidade, Autenticidade, Legalidade, Finalidade, Adequação, Necessidade, Livre acesso, Qualidade dos dados, Transparência, Segurança, Prevenção, Não discriminação, Responsabilização e prestação de contas.

II - Esta Política de Segurança da Informação do IPSM tem respaldo legal nas legislações a seguir: Lei Federal nº 12.965/2014, Lei Federal nº 12.527/2011, Lei Federal nº 13.460/2017, Lei Federal nº 13.709/2018, Decreto Estadual nº 47.974/2020, Decreto Estadual nº 45.969/2022, Decreto Estadual nº 46.226/2013, Decreto Estadual nº 45.241/2009, Decreto Estadual nº 48.383/2022, Resolução SEPLAG Nº 084/ 2022.

III - Em casos omissos, deverá ser observado a Resolução SEPLAG nº 084, DE 11 de novembro de 2022 e legislações da Tecnologia da Informação vigente, do Estado de Minas Gerais.

IV - O IPSM entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados aos seus beneficiários.

V - O IPSM compreende que as manipulações das informações passam por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

VII - Dessa forma, o IPSM estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção às informações da organização ou sob sua responsabilidade, em conformidade com a Resolução SEPLAG nº 084/2022.

VIII - Para os fins desta Portaria, considera-se:

a) **IPSM:** Instituto de Previdência dos Servidores Militares do Estado de Minas Gerais;

b) **ATI:** Assessoria de Tecnologia da Informação;

c) **GRH:** Gerência de Recursos Humanos;

d) **DRH:** Departamento de Recursos Humanos;

e) **DLT:** Departamento de Logística e Transporte;

f) **Ameaça**: causa potencial de um incidente, que pode vir a prejudicar o IPSM;

g) **Ativo:** tudo aquilo que possui valor para o IPSM;

h) **Ativo de informação:** patrimônio intangível do IPSM, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas ao **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS** por parceiros, beneficiários, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional do IPSM ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídias eletrônicas transitadas dentro e fora de sua estrutura física;

i) **Comitê Gestor de Segurança Da Informação – CGSI:** grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do IPSM, que tem por finalidade tratar questões ligadas à Segurança da Informação;

j) **Confidencialidade:** propriedade dos ativos da informação do IPSM, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas;

k) **Controle:** medida de segurança adotada pelo IPSM para o tratamento de um risco específico;

l) **Disponibilidade:** propriedade dos ativos da informação do IPSM, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas;

m) **Gestor da Informação:** usuário da informação que ocupe cargo especifico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação;

n) **Incidente de segurança da informação:** um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações do IPSM;

o) **Integridade:** propriedade dos ativos da informação do IPSM, de serem exatos e completos;

p) **Risco de segurança da informação:** efeito da incerteza sobre os objetivos de segurança da informação do IPSM;

q) **Segurança da informação:** a preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do IPSM;

r) **Usuário da informação:** empregados com vínculo empregatício de qualquer área do IPSM ou terceiros alocados na prestação de serviços o IPSM, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação do **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DE MINAS GERAIS** para o desempenho de suas atividades profissionais;

s) **Vulnerabilidade:** causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações do IPSM.

IX - Esta política como propósito:

a) Estabelecer diretrizes e normas de Segurança da Informação que permitam aos servidores, colaboradores, beneficiários e a todos que utilizam dos serviços prestados pelo **IPSM** adotarem padrões de comportamento seguro, adequados às metas e necessidades do IPSM, aplicando também a fornecedores no desempenho de alguma atividade internamente ao ambiente lógico do IPSM;

b) Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

c) Resguardar as informações do IPSM, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

d) Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus servidores, colaboradores, beneficiários e parceiros;

e) Minimizar os riscos de perda, da confiança de beneficiários ou qualquer outro impacto negativo nos serviços prestados pelo IPSM como resultado de falhas de segurança da informação.

X - Esta política se aplica a todos os usuários da informação do IPSM, incluindo qualquer indivíduo ou organização que possui ou possuiu vinculo com o IPSM, tais como servidores ativos e aposentados, estagiários, beneficiários, empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuem ou virão a possuir acesso às informações do IPSM e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura do IPSM.

XI - O objetivo da Gestão de Segurança da Informação do IPSM é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a instituição.

XII - A Diretoria do IPSM e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação no IPSM. Desta forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades do IPSM.

XIII - É política do IPSM:

a) Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação do IPSM sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;

b) Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: servidores, colaboradores, empregados, beneficiários, terceiros contratados e, onde for pertinente;

c) Garantir a educação e conscientização sobre as práticas adotadas pelo IPSM de segurança da informação para servidores, colaboradores, terceiros contratados e, onde for pertinente, beneficiários;

d) Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

e) Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e , quando necessário, comunicando as autoridades apropriadas;

f) Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

g) Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

XIV - Do Comitê Gestor de Segurança da Informação – CGSI:

a) Fica constituído o COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO, contando com a participação de, pelo menos, um representante da diretoria e um membro sênior das seguintes áreas: ATI - Assessoria de Tecnologia da Informação, Gerência de Recursos Humanos, Procuradoria e Representante da Previdência e Saúde.

b) É responsabilidade do CGSI:

1) Analisar, revisar e propor a aprovação de políticas e normas e diretrizes relacionadas à segurança da informação;

2) Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

3) Garantir que as atividades de segurança da informação sejam executadas em conformidade com a Política de Segurança da Informação do IPSM e seus anexos;

4) Promover a divulgação da PSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do IPSM;

5) Avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria;

6) Avaliar, aprovar ou negar solicitações para uso de dispositivos pessoais no ambiente corporativo, bem como avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria;

7) Elencar, em conjunto coma a Diretoria do IPSM, nos termos da Política de Segurança da Informação, servidores para analisar as violações de segurança, ocorridas no IPSM, bem como auxiliar a Diretoria na elaboração da resposta ao incidente.

XV - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:

a) Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CGSI;

b) Apoiar o CGSI em suas deliberações;

c) Elaborar e propor ao CGSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PSI;

d) Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

e) Tomar as ações cabíveis para se fazer cumprir os termos desta política;

f) Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado;

g) Manter os sistemas computacionais e de comunicação em conformidade com a Política de Segurança da Informação;

h) Disponibilizar os recursos necessários à implantação da Política de Segurança da Informação;

i) Manter os dados cadastrais dos usuários da rede corporativa, bem como do correio eletrônico, atualizados;

j) Reportar incidentes de segurança da informação à área responsável;

k) Monitorar os logs dos sistemas;

l) Acompanhar a realização de manutenção, corretiva ou preventiva, dos servidores e subsistemas de armazenamento da rede corporativa do IPSM quando a manutenção for realizada por terceiros no ambiente do IPSM;

m) Prestar suporte ao usuário quando solicitado;

n) Solicitar apoio e consultoria de segurança à área responsável pela Segurança da Informação quando se fizer necessário, caso houver;

o) Solicitar a assinatura do Termo de Confidencialidade do usuário;

p) Instalar e configurar os Computadores nas estações de trabalho;

q) Manter um inventário atualizado dos computadores e dos softwares;

r) Desenvolver e manter um padrão de instalação e configuração dos computadores, aderente aos critérios estabelecidos pelo IPSM;

s) Configurar os programas de computador e equipamentos para garantir a utilização dos critérios relativos às senhas de acesso definidos;

t) Manter o antivírus, anti-spam e as correções de segurança dos servidores e computadores atualizados;

u) Lacrar os computadores;

v) Disponibilizar e administrar a infraestrutura necessária para armazenamento de dados;

w) Disponibilizar e administrar os recursos de acesso à Internet;

x) Monitorar o uso da Internet;

y) Registrar os acessos indevidos à Internet;

z) Orientar os usuários em relação à proteção adequada dos dispositivos móveis;

aa) Configurar os dispositivos móveis disponibilizados para os usuários do IPSM;

bb) Instalar, homologar, manter, atualizar e configurar todos os servidores, subsistemas de armazenamento e programas de computador que componham as soluções de backup e restore utilizadas no IPSM;

cc) Manter a documentação dos servidores, subsistemas de armazenamento, e programas de computador diretamente vinculados às soluções de backup e restore;

dd) Realizar o backup e a remoção das informações armazenadas nos servidores e subsistemas de armazenamento da rede corporativa do IPSM, no caso de manutenção externa ao IPSM;

ee) Definir os recursos e ferramentas que serão utilizados em cada procedimento de backup e restore;

ff) Documentar os procedimentos de backup e restore;

gg) Eliminar e substituir as mídias de backup e restore próximas de perderem sua funcionalidade segundo a vida útil informada pelo fornecedor;

hh) Eliminar o conteúdo das mídias que serão descartadas;

ii) Executar os procedimentos de backup e restore;

jj) Gerenciar e controlar os recursos computacionais e as mídias utilizadas pelos sistemas de backup e restore do IPSM;

kk) Manter mapa atualizado das mídias e seus conteúdos para todos os procedimentos de backup e restore do IPSM;

ll) Planejar junto às áreas solicitantes os procedimentos de backup e restore;

mm) Realizar testes de validação e desempenho das cópias de segurança realizadas;

nn) Disponibilizar os recursos necessários para a execução das funções de auditoria;

oo) Garantir a proteção adequada das trilhas de auditoria;

pp) Aprovar e registrar a utilização das ferramentas de monitoramento e acesso às estações de trabalho;

qq) Analisar e despachar os expedientes relativos a solicitações de usuários encaminhadas pelos respectivos responsáveis por suas unidades;

rr) Administrar o acesso remoto à rede do IPSM;

ss) Definir os softwares autorizados que deverão ser instalados nas estações de trabalho;

tt) Administrar as redes corporativas do IPSM;

uu) Manter a documentação da topologia da rede atualizada e controlar o acesso ao seu conteúdo;

vv) Prover o ambiente físico necessário para instalação dos roteadores e switches;

ww) homologar e administrar os roteadores e switches do IPSM;

xx) Manter a documentação (topologia, configurações, etc) dos roteadores e switches atualizada;

yy) Administrar as regras dos firewalls;

zz) Instalar, configurar e manter os ambientes operacionais dos firewalls - sistema operacional nos servidores, bem como os produtos e as correções e atualizações de versão;

aaa) Aplicar, anualmente, os controles disponibilizados pela ferramenta de gestão de riscos nos ativos em que estejam instalados os firewalls;

bbb) Manter atualizadas as documentações (configurações) relativas aos firewalls;

ccc) Disponibilizar a infraestrutura necessária para o funcionamento da solução de network IDS/IPS;

ddd) Instalar e administrar o network IDS/IPS;

eee) Analisar periodicamente as logs dos Networks IDS em busca de incidentes de Segurança da Informação;

fff) Avaliar, o desempenho do network IDS/IPS em relação à quantidade de ataques detectados, falsos positivos (alarme falso), carga da rede, entre outros;

ggg) Manter a documentação do network IDS/IPS atualizada;

hhh) Instalar, homologar, manter e configurar todos os equipamentos de conectividade que componham as soluções de backup e restore utilizadas no IPSM;

iii) Definir e implementar rotina automatizada para a cópia das configurações e dados dos equipamentos de conectividade para um servidor de arquivos contemplado por uma das rotinas de backup/restore;

jjj) Analisar e emitir parecer sobre as solicitações da área de segurança da informação, quando houver e se solicitado;

kkk) Atualizar os controles da ferramenta de análise de risco de Segurança da Informação, caso houver;

lll) Avaliar e aplicar, para as situações consideradas críticas, os controles existentes na ferramenta de análise de risco de Segurança da Informação;

mmm) Elaborar e manter atualizado um procedimento de instalação e configuração da rede;

nnn) Administrar a cessão, a alteração, o bloqueio e o cancelamento de acessos à rede corporativa;

ooo) Revisar os direitos de acesso dos usuários da rede corporativa e realizar as alterações necessárias;

ppp) Revisar, os direitos de acesso com privilégios de administrador e realizar as alterações necessárias;

qqq) Definir, homologar, implementar e disponibilizar a infraestrutura e os mecanismos de segurança para utilização da rede wireless;

rrr) Realizar análise de risco na rede wireless;

sss) Disponibilizar relatório as conexões remotas realizadas;

ttt) Solicitar a autorização para movimentação patrimonial de ativos (hardware) ao DLT.

XVI - É responsabilidade dos Gestores da Informação:

a) Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo IPSM;

b) Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pelo IPSM;

c) Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;

d) Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

e) Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo IPSM.

XVII - É responsabilidade dos Usuários da Informação:

a) Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

b) Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, suas normas e procedimentos a ATI ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;

c) Comunicar à ATI qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais do IPSM;

d) Assinar o Termo de Uso de Sistemas de Informação do IPSM, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

e) Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de

segurança, conforme definido no item sanções;

f) Sugerir medidas que possam elevar os níveis de segurança das instalações na sua área de atuação;

g) Responder pelo uso de seu login de acesso aos sistemas e serviços do IPSM;

h) Zelar pelas informações, sistemas, serviços e recursos de tecnologia da informação sob sua responsabilidade;

i) Não realizar alterações na configuração do computador sem autorização;

j) Utilizar adequadamente os recursos computacionais;

k) Conduzir adequadamente o uso da Internet, respeitando direitos autorais, regras de licenciamento de softwares, direitos de propriedade e privacidade;

l) Alterar a senha no momento em que receber as informações da criação de sua conta;

m) Manter sigilo de seu login e de sua senha de acesso aos sistemas e serviços do órgão ou entidade;

n) Trocar a senha sempre que houver indícios de comprometimento do sistema ou da própria senha;

o) Guardar as mídias removíveis, contendo dados, em armários com chaves;

p) Eliminar os arquivos desnecessários armazenados nos servidores da rede do IPSM;

q) Responder pelo uso de dispositivos particulares no ambiente do IPSM;

r) Solicitar à Chefia imediata a utilização e a conexão do dispositivo móvel na rede corporativa justificando a sua necessidade;

s) Evitar armazenar informações confidenciais em dispositivos móveis usados fora do órgão ou entidade. Havendo necessidade, tais informações deverão ser transferidas para um local de armazenamento seguro logo que possível;

t) Ser responsável pelos dispositivos móveis, e pelos dados armazenados nos mesmos, disponibilizados para uso dentro e fora das instalações do IPSM;

u) Não deixar os dispositivos móveis desprotegidos em locais de alto risco, tais como locais públicos, eventos, hotéis, veículos, dentre outros;

v) Apresentar em caso de furto, roubo ou extravio do dispositivo móvel a Ocorrência Policial, no prazo máximo de 48 horas do fato ocorrido, à área responsável pelo patrimônio do IPSM;

w) Apresentar o dispositivo móvel para a área responsável pelo atendimento ao usuário, quando requisitado, ou ao cessar as atividades que motivaram sua solicitação;

x) Zelar pela guarda do dispositivo de armazenamento do certificado digital e pela senha de acesso ao dispositivo;

y) Requisitar a revogação do certificado digital caso ele seja perdido, roubado ou extraviado, informando imediatamente o fato à área responsável;

XVII - O usuário que não cumprir as normas estabelecidas nessa Política estará sujeito às penalidades previstas em Lei.

XVIII - Será avaliado pelo Comitê Gestor de Segurança da Informação - CGSI do IPSM, a ser criado por Portaria interna do Diretor-Geral do IPSM, onde o CGSI, informará autoridade competente, que verificará a gravidade dos fatos, e, nos casos de servidores podendo gerar um processo interno para avaliação.

XIX - O descumprimento do disposto nesta Política sujeitará o servidor, o prestador de serviço terceirizado e o estagiário às sanções e às penalidades previstas em lei, assegurados o contraditório e a ampla defesa.

XX - Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano o IPSM ou a outrem, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes pelos Órgãos Competentes, sem prejuízo aos termos descritos nesta política.

XXI - Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

XXII - As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança constantes a seguir nesta Portaria, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças.

XXIII - Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do IPSM adotar, sempre que possível outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações do IPSM.

XIV - As normas a seguir complementam a Política de Segurança da informação - PSI do IPSM.

Art. 3º - **DA NORMA DE USO ACEITÁVEL DE ATIVOS DE INFORMAÇÃO - N-SI-002**

I - A Norma de segurança da informação **N-SI-002** complementa Política de Segurança da Informação, definindo as diretrizes para o uso aceitável de ativos de informação do **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS** por seus usuários autorizados.

II - Seu propósito é estabelecer diretrizes para o uso aceitável, entendido como seguro, dos ativos de informação do IPSM por seus usuários autorizados.

III Esta norma obedece ao escopo definido na Política de Segurança da Informação, constante no Art. 2º desta Portaria.

IV - Uso de equipamento computacional:

a) O IPSM fornece para seus usuários equipamentos para o desempenho exclusivamente de suas atividades profissionais;

b) Todo usuário deve observar as seguintes disposições quanto ao uso de equipamentos de propriedade do IPSM;

c) Os equipamentos disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais são de propriedade do IPSM, sendo expressamente proibida a utilização para fins particulares;

d) A alteração e/ou a manutenção de qualquer equipamento de propriedade do IPSM é uma atribuição específica da ATI que, ao seu critério exclusivo, poderá delegar formalmente outro responsável. Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos;

e) Os equipamentos do IPSM devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado;

f) Computadores de mesa (*desktops*) ou móveis (*notebooks*) e (tablet) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado, exceto quando existir uma justificativa plausível em virtude de atividades de trabalho;

g) A desconexão (*log off*) da rede deverá ser efetuada nos casos em que o usuário não for mais utilizar o equipamento ou venha a ausentar-se por um período prolongado;

h) O bloqueio de tela protegido por senha deverá ser ativado sempre que o usuário se afastar do computador de mesa ou móvel que esteja utilizando;

i) Os equipamentos disponibilizados pelo IPSM, para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado e original quando no desligamento ou término da relação do usuário com do IPSM, sendo que para equipamentos considerados permanentes, a chefia imediata deve solicitar sua devolução, para retirada do material do mapa carga junto ao DLT;

j) O DLT solicitará a ATI a avaliação de equipamentos informacionais para finalização da Baixa de carga patrimonial. Constatado qualquer dano aos equipamentos do IPSM será devidamente analisado pela ATI. Havendo a constatação de que tal dano decorreu de mau uso do usuário, caberá a IPSM exercer seu direito de reparação ao prejuízo, através da tomada das medidas administrativas cabíveis;

h) Para avaliação do material, o usuário deverá realizar abertura do Chamado no site do IPSM, para avaliação do material pela ATI. Será realizado agendamento de data e hora. Será elaborado parecer técnico

(laudo do material) pela área responsável do IPSM onde constará o estado do material. A ATI enviará o laudo para o DLT para demais providências cabíveis;

i) Caso seja detectado mau uso ou avariais no equipamento, o usuário será notificado para maiores explicações;

j) Caso o equipamento com avariais ou defeito esteja impossibilitado para uso, o DLT solicitará à ATI uma avaliação mais minuciosa do defeito e em casos específicos de defeitos do hardware, será enviado para uma assistência técnica especializada para emissão de um relatório circunstanciado sobre o defeito do equipamento;

k) Comprovado o mau uso do equipamento, o DLT acionará o usuário e o mesmo poderá:

1 - Procurar um técnico de sua confiança para realização do conserto, por sua conta e risco, sendo que o equipamento após o conserto passará por nova avaliação do DLT e da ATI, com emissão de novo laudo;

2 - Caso em que o usuário não opte pelo conserto, ele terá a opção de realizar a compra de um material igual ou superior, com as mesmas características técnicas, equivalente, capaz de atender às suas necessidades de forma satisfatória o IPSM. O aparelho deve ser novo, sem uso e deverá passar por nova emissão de avaliação técnica do IPSM;

3 - Autorizado pelo Usuário, o IPSM solicitará o conserto do notebook sendo que os custos do conserto e troca de peças ficará a cargo do usuário que casou dano ao material.

l) Em caso de perda ou furto de equipamento de propriedade do IPSM, o usuário deverá comunicar imediatamente o DLT e a ATI para que possam ser tomadas as medidas cabíveis de revogação de acessos a rede do IPSM bem como de outros sistemas que o Usuário possua e ainda deverá realizar boletim de ocorrência apresentando o respectivo documento no momento da comunicação ao DLT/ATI;

j) A seu critério exclusivo o IPSM poderá permitir a utilização de equipamento particular para o desempenho de atividades profissionais, devendo os mesmos passar por inspeção da ATI de forma a garantir adequação aos requisitos e controles de segurança adotados pela empresa;

k) Não é permitida a conexão de equipamentos particulares na rede administrativa do IPSM, seja em segmentos cabeados ou sem fio, sem autorização prévia formal e inspeção do equipamento pela ATI;

V - Dispositivos de Armazenamento Removível:

a) O IPSM poderá, ao seu critério exclusivo, fornecer aos seus usuários dispositivos móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, devendo ser observadas além das diretrizes acima, as seguintes;

b) O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda;

c) O dispositivo será de uso e responsabilidade de seu usuário, nos termos do formulário de recebimento do DLT (Termo de Cessão de Uso), assinado no momento de entrega;

d) O Usuário, na utilização dos dispositivos móveis fora do ambiente do IPSM, deverá estar alerta e ter uma conduta discreta e zelando pela material, dando preferência para compartimentos de armazenamento resistentes;

e) A instalação de ferramentas de proteção para dispositivos móveis é realizada exclusivamente pela ATI e é obrigatória para todos os equipamentos corporativos; e

f) Em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deverá comunicar imediatamente o DLT e a ATI para que possam ser tomadas as medidas cabíveis e deverá realizar boletim de ocorrência apresentando o respectivo documento no momento da comunicação ao DLT.

VI - Identificação digital:

a) O IPSM poderá, ao seu critério exclusivo ou conforme legislação pertinente, fornecer certificados digitais para usuários que execução de atividades profissionais específicas, devendo ser observadas as seguintes diretrizes;

b) Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo;

c) O usuário deverá informar a ATI sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;

d) O usuário desligado ou em processo de desligamento terá o certificado digital expedido pelo IPSM imediatamente revogado;

f) É de responsabilidade da ATI prover a atualização de todos os pontos de verificação com as respectivas listas de revogação.

VII - Equipamentos de impressão e reprografia:

a) O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse do IPSM ou que estejam relacionados com o desempenho das atividades profissionais do usuário;

b) O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de impressão e reprografia;

c) O usuário deve retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações do IPSM, classificadas como de uso interno ou confidencial;

d) A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;

e) Não será admissível, o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais ou pessoais, devendo as mesmas ser descartadas de acordo com os procedimentos adotados pelo IPSM.

VIII - Segurança física dos ativos de informação:

a) As instalações de processamento das informações do IPSM serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, ou os danos e quaisquer interferências de origem humana ou natural;

b) Deverá ser observado as seguintes disposições específicas quanto à segurança física;

c) Crachás de identificação de terceiros e autorizado, inclusive temporários expedidos pelo IPSM, são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;

d) Estando em áreas sensíveis, os colaboradores devem portar crachás de identificação que exibam claramente seu nome e fotografia. Terceiros autorizados devem portar crachás temporários pelo IPSM identificando claramente que os mesmos não são colaboradores;

e) Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;

f) É proibida qualquer tentativa de se obter ou permitir o acesso aos indivíduos não autorizado a áreas sensíveis do IPSM;

g) É resguardado ao IPSM o direito de monitorar seus ambientes físicos. Para isso será utilizado sistema de circuito fechado de televisão em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida, e serão utilizadas exclusivamente para verificação interna, não podendo ser solicitada para outro fim, exceto em casos previstos em lei;

h) Não é permitido consumir qualquer tipo de alimento, bebida ou fumar em áreas apontadas como sensíveis, incluindo computadores e seus periféricos, bem como quaisquer dispositivos móveis de responsabilidade do IPSM.

IX - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:

a) Estabelecer e manter atualizados os procedimentos complementares a esta norma;

b) Comunicar ao CGSI eventuais tentativas, bem sucedidas ou não, de desvio de conduta dos termos dessa norma.

Art. 4º - **GESTÃO DE IDENTIDADE DE CONTROLE DE ACESSO - N-SI-003**

I - A Norma de segurança da informação **N-SI-003** complementa Política de Segurança da Informação, definindo as diretrizes para garantir que o acesso aos ativos de informação ou sistemas de informação do **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS** garanta níveis adequados de proteção.

II - Seu propósito é estabelecer diretrizes para gestão de identidade e acesso aos ativos e sistemas de informação do IPSM.

III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, constante no Art. 2º desta Portaria.

IV - Acesso a ativos e sistemas de informação:

a) O IPSM fornece aos seus usuários autorizados contas de acesso aos sistemas cadastrados que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa;

b) As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;

c) Toda conta de acesso é pessoal do usuário a qual foi delegada e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso.

d) Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro aos ativos e serviços de informação, incluindo:

1 - Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pelo IPSM;

2 - Não utilizar sua conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pelo IPSM;

3 - Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;

4 - Informar imediatamente a ATI caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais do IPSM.

e) Usuários que tem acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica fornecida pelo IPSM que pode ser um cartão de acesso, biometria ou uma conta de criada para acesso aos sistemas – com privilégios administrativos, para este propósito. A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia;

f) Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração e notificação pela Autoridade Competente que analisará a aplicação das sanções previstas na Política de Segurança da Informação, conforme Norma P-SI-001, e que serão submetidos à autoridade competente para medidas cabíveis citadas na mesma.

V - Senha de acesso:

a) As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais do IPSM são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;

b) O IPSM adota os seguintes padrões para geração de senhas de acesso a seus ativos/serviços de informação ou recursos computacionais:

c) A equipe da ATI será responsável por fornecer senhas de acesso inicial ao usuário, que deverá proceder com a troca imediata da mesma;

d) As senhas terão prazo de validade a ser definido pela ATI. Passado este prazo, os sistemas solicitarão automaticamente a troca da senha;

e) As senhas associadas às contas com privilégio não-administrativo serão compostas usando uma quantidade mínima de 08 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres

especiais;

f) As senhas associadas às contas que possuem privilégio administrativo serão compostas usando uma quantidade mínima de 08(oito) dígitos, combinando letras maiúsculas e minúsculas, números;

g) Após 05 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário será bloqueada, assim permanecendo assim por, no mínimo, 30 (trinta) minutos;

h) Quando efetuada uma troca da senha, o usuário não poderá realizar nova alteração dentro de um prazo mínimo de 7 (sete) dias. Caso seja necessário realizar alteração dentro deste período, o usuário deverá solicitar o apoio da ATI;

i) Quando criada uma nova senha, usuários devem estar atentos as seguintes recomendações:

1 - Não utilizar nenhuma parte de sua credencial na composição da senha;

2 - Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;

3 - Não utilizar repetição ou sequencia de caracteres, números ou letras;

4 - Qualquer parte ou variação do nome – IPSM;

5 - Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

VI - Autorização de acesso (privilégios de acesso):

a) A autorização e o nível permitido de acesso aos ativos/serviços de informação do IPSM é feita com base em perfis que definem o nível de privilégio dos usuários;

b) O acesso à ativos/serviços de informação é fornecido a critério do IPSM, que define permissões baseadas nas necessidades laborais dos usuários;

c) Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador. Solicitações deverão ser encaminhadas a ATI;

d) Para criação de contas de acessos a sistemas ou a acesso à rede do IPSM, a Chefia imediata deve solicitar a ATI, por intermédio de abertura de chamado no Site do IPSM, contendo os seguintes dados do Colaborador:

1- Nome completo;

2- Diretoria, Assessoria, Gerência ou Departamento que o Colaborador ficará alocado;

3- Telefone/Ramal;

4- Matricula ou Masp;

VII - Os usuários devem, ainda, observar as seguintes diretrizes:

a) A seu critério exclusivo, o IPSM poderá ativar uma cota para armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto (nuvem). Caso o usuário necessite de mais espaço, deverá realizar uma solicitação à ATI através dos canais formais e institucionais estabelecidos;

b) É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse do IPSM tanto na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem);

c) Os arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) do IPSM pessoais podem ser excluídos, após aviso prévio ao usuário, pois todos são monitorados e auditados pela ATI. Caso sejam detectados arquivos pessoais ou em desacordo com a Política de Segurança do IPSM, será solicitado pela ATI a remoção ou exclusão pelo dono do arquivo.

VIII - É responsabilidade da ATI – Assessoria de Tecnologia da Informação:

a) Autorizar a concessão e revogação de acesso a ativos/sistemas de informação sob sua responsabilidade;

b) Autorizar a concessão e o controle de acesso administrativo a ativos/sistemas de informação sob sua responsabilidade;

c) Realizar a revisão periódica de autorizações de acesso e credenciais de acesso a ativos/sistemas de informação sob sua responsabilidade;

d) Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários de colaboradores, terceiros/prestadores de serviços;

e) Conceder, quando autorizado, o acesso aos usuários de colaboradores, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;

f) Revogar, quando solicitado, o acesso dos usuários de colaboradores, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;

g) Apoiar a revisão periódica da validade de credenciais de acesso aos ativos/sistemas de informação dos usuários e colaboradores, terceiros/prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

IX - É responsabilidade do Departamento de Recursos Humanos - DRH:

a) Realizar o registro do desligamento dos colaboradores do IPSM no sistema destinado a essa finalidade para que a ATI receba a notificação e proceda com a exclusão devida dos acessos;

b) Apoiar a gestão de identidades dando a devida manutenção no sistema destinado a essa finalidade enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posição no IPSM;

c) Apoiar a revisão periódica da validade de credenciais de acesso aos ativos/sistemas de informação fornecendo informações sobre os colaboradores.

X- É responsabilidade dos Gerentes e Chefes de Departamento:

a) Solicitar a ATI através dos canais formais e institucionais estabelecidos a concessão e a revogação de acessos de novos colaboradores, servidores ou empregados, colaboradores e servidores que necessitem de novos acessos conforme mudanças em suas atividades laborais, ou por desligamento do setor ou do IPSM;

b) Solicitar ATI através dos canais formais e institucionais estabelecidos a concessão e a revogação de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso aos ativos/sistemas de informação ou por desligamento do setor ou do IPSM;

c) Informar a equipe da ATI quando ao encerramento do contrato com terceiros/prestadores de serviços contratados e colaboradores em geral que tenham a ativos/sistemas de informação.

Art. 5º - **DO ACESSO A INTERNET E COMPORTAMENTO EM MÍDIAS SOCIAIS - N-SI-004**

I - A Norma de segurança da informação **N-SI-004** complementa Política de Segurança da Informação, definindo as diretrizes para utilização segura do acesso à internet fornecido pelo **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS BRASIL** e do comportamento de colaboradores em mídias e redes sociais.

II - A norma tem propósito de estabelecer diretrizes para utilização segura do acesso à internet fornecido pelo IPSM e do comportamento de colaboradores em mídias e redes sociais.

III - Esta norma obedece ao escopo definido na Política de Segurança da Informação.

IV - Acesso à internet:

a) O IPSM fornece acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais . O usuário deverá utilizar a Internet em conformidade com a lei, a ordem pública e o Código de Conduta Ética do Agente Público e da Alta Administração Estadual;

b) O acesso à internet pode ser fornecido tanto através da rede corporativa do IPSM, quanto através da disponibilização de serviços de internet móvel, prestados por terceiros, contratados pelo IPSM;

c) O Acesso à internet por meio da rede wifi será disponibilizado aos colaboradores, conforme, solicitação dos Chefes de Departamentos, Gerentes, Assessores e Diretores;

d) Toda informação que é acessada, transmitida, recebida ou produzida através do acesso à internet fornecido pelo IPSM está sujeita ao monitoramento;

e) Caso o usuário esteja utilizando de forma excessiva a banda da internet, o mesmo será avisado e notificado pela ATI, para esclarecimento;

f) Na identificação da conduta irregular por parte do usuário, será submetido à Autoridade Competente para medidas cabíveis citadas nesta Política de Segurança da Informação;

g) Durante o monitoramento realizado pela ATI do IPSM, se resguarda o direito de efetuar o bloqueio da conta do Usuário, para fins de segurança;

h) Durante o acesso à Internet fornecido pelo IPSM não será permitido o *download*, o *upload*, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento e/ou a cópia de qualquer conteúdo relacionado expressa ou subjetivamente, direta ou indiretamente, com:

1 - Qualquer espécie de exploração sexual;

2 - Qualquer forma de conteúdo adulto, erotismo, pornografia;

3 - Qualquer tipo de Pornografia infantil;

4 - Qualquer forma de ameaça, chantagem e assédio moral ou sexual;

5 - Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;

6 - Preconceito baseado em cor, sexo, orientação sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;

7 - Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam essas lícitas ou não;

8 - A prática e/ou a incitação de crimes ou contravenções penais;

9 - A prática de propaganda política nacional ou internacional;

10 - A prática de quaisquer atividades comerciais desleais;

11 - Qualquer conteúdo protegido por direitos autorais;

12 - O desrespeito a imagem ou aos direitos de propriedade intelectual do IPSM;

13 - A disseminação de códigos maliciosos e ameaças virtuais;

14 - Tentativa de expor a infraestrutura computacional do IPSM a ameaças virtuais;

15 - Divulgação não autorizada de qualquer informação do IPSM**,** classificada como confidencial ou de uso interno;

16 - Uso de sites ou serviços que busquem contornar controles de acesso à internet.

V - Publicação de Conteúdo no Site do IPSM:

a) A publicação de conteúdo no site IPSM e de **responsabilidade específica da ATI**, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da organização;

VI - É responsabilidade da ATI - Assessoria de tecnologia da informação:

a) Controlar e monitorar qualquer tipo de acesso à internet fornecido pelo IPSM;

b) Reportar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso a internet à Diretoria.

Art. 6º - **DO USO DE SERVIÇOS DE EMAIL E COMUNICADORES INSTANTÂNEOS - N-SI-005**

I - A Norma de segurança da informação **N-SI-005** complementa Política de Segurança da Informação, definindo as diretrizes para utilização dos serviços de e-mail e comunicadores instantâneos fornecidos pelo **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS.**

II - O propósito é Estabelecer diretrizes para utilização segura dos serviços de e-mail e comunicadores instantâneos fornecidos pelo IPSM.

III - Esta norma obedece ao escopo definido na Política de Segurança da Informação.

IV - Serviço de E-mail:

a) O IPSM fornece o serviço de e-mail para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais;

b) Não é permitido o uso de qualquer serviço de e-mail, que não seja o oficialmente fornecido pelo IPSM;

c) Quando o usuário fizer uso do serviço de e-mail do IPSM, não é permitido:

1 - Utilizar do serviço de e-mail em caráter pessoal ou para fins que não sejam de interesse do IPSM;

2 - Utilizar de termos ou palavras de baixo calão na redação de mensagens;

3 - Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para endereços eletrônicos que não fazem parte do domínio corporativo do IPSM, excetuando-se quando expressamente autorizados;

4 - Inscrever o endereço de e-mail do IPSM em listas de distribuição e grupos de discussão que não estejam relacionadas com atividades laborais ou do interesse da organização;

5 - Fazer uso de qualquer técnica de falsificação ou simulação de falsa identidade e manipulação de cabeçalhos de e-mail. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas onde o Comitê Gestor de Segurança da Informação, notificará à autoridade competente que analisará a aplicação das sanções e punições previstas na Política de Segurança da Informação, e, nos casos de servidores podendo gerar um processo interno para avaliação;

6 - Tentar a interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;

7 - Utilizar o serviço de e-mail para o envio de mensagens indesejadas (spam) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de e-mail;

8 - Usar o serviço de e-mail para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;

9 - Usar o envio de material e mensagens de natureza ou com conteúdo racista, profana, obscena, intimidadora, difamatória, ilegal, ofensiva, abusiva, não ética, comercial, estritamente pessoal, de entretenimento, spam, com caráter eminentemente associativo, sindical, religioso, político e partidário, assim como qualquer outro que possa infringir a legislação vigente;

10 - Usar o serviço de e-mail para disseminar ou transmitir mensagens com conteúdo de cunho de propriedade autoral;

d) O serviço de e-mail do IPSM é continuamente monitorado para segurança, para fins de auditoria e verificação de sua devida utilização;

e) Na ocorrência de evidências de uso irregular do serviço de correio eletrônico, o IPSM efetuará registro do incidente de segurança da informação e notificará a Autoridade Competente, que decidirá sobre o processo de abertura de sindicância administrativa, com auditoria nas contas dos usuários sob suspeita, a fim de averiguar e garantir a segurança de toda a infraestrutura de tecnologia da informação e comunicação, bem como resguardar os objetivos, com base nas legislações vigentes;

f) O monitoramento do serviço de e-mail do IPSM tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como cumprir à legislação em vigor;

h) Na identificação da conduta irregular por parte do usuário, será submetido à Autoridade Competente para medidas cabíveis citadas nesta Política de Segurança da Informação;

i) Durante o monitoramento realizado pela ATI do IPSM, se resguarda o direito de efetuar o bloqueio da conta do Usuário, para fins de segurança;

j) O IPSM adota um padrão para criação dos endereços de E-mail sendo composto pelo primeiro nome do empregado, seguido por pontuação e seu último sobrenome, conforme exemplo a seguir:

1 - Nome completo do empregado: Marco de Araújo Soares;

2 - Email: marco.soares@ipsm.gov.br;

k) Casos de endereços de e-mail coincidentes ou que possam ocasionar cacofonias e situações vexatórias poderão ser alterados para seguir um modelo fora do padrão adotado pelo IPSM, devendo primeiramente ser revisados pela equipe da ATI;

l) Os usuários do serviço de e-mail do IPSM devem adotar a assinatura padrão, formatada de acordo com o seguinte:

1 - Modelo:

- Nome Completo
- Nome do departamento | sigla do departamento
- Nome da diretoria | sigla da diretoria
- Nome do Instituto completo
- Endereço do Instituto completo
- Telefone de contato do Instituto | site do Instituto

2 - Exemplo:

- Marco de Araújo Soares
- Assessoria de Tecnologia da Informação | ATI
- Diretoria Geral | DG
- IPSM -Instituto de Previdência dos Servidores Militares
- Rua Paraíba, 576 | 30130-140 | Belo Horizonte - MG | Brasil
- Tel.: +55 31 3269-20XX | www.ipsm.gov.br

3 - Ao final do e-mail, após a assinatura, deverá ser exibido o seguinte aviso de confidencialidade:

- *O endereço (@ipsm.gov.br) é exclusivamente para as atividades profissionais de recepção e distribuição de informações. Lembre-se que o e-mail fornecido pelo IPSM é uma ferramenta de trabalho e pertencente à instituição.*
- *Esta mensagem é destinada exclusivamente a seu destinatário e pode conter informações privadas, privilegiadas e confidenciais. Se você a recebeu por engano, por favor, notifique imediatamente o remetente e elimine-a de seu computador. Qualquer disseminação, distribuição ou cópia desta comunicação é estritamente proibida.*
- *Antes de Imprimir, pense sobre sua responsabilidade social. Menos papel, mais árvores!*

j) Para criação de contas de e-mails, a Chefia imediata deve solicitar a ATI, por intermédio de abertura chamado no Site, contendo os seguintes dados do Colaborador:

1 - Nome completo;

2 - Diretoria, Assessoria, Gerência ou Departamento que o Colaborador ficará alocado;

3 - Telefone/Ramal;

4 - Matricula ou Masp;

V - Serviços de Comunicadores instantâneos:

a) O IPSM disponibiliza o serviço de comunicadores instantâneos para seus usuários autorizados, exclusivamente para o desempenho de suas atividades profissionais;

b) Não é permitido o uso de qualquer serviço de comunicadores instantâneos, que não sejam oficialmente disponibilizados ou liberados pelo IPSM;

c) Quando o usuário fizer uso do serviço de comunicadores instantâneos do IPSM, não é permitido:

1 - Utilizar do serviço de comunicadores instantâneos em caráter pessoal ou para fins que não sejam de

interesse do IPSM;

2 - Utilizar de termos ou palavras de baixo calão na redação de mensagens;

3 - Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para pessoas ou entidades que não fazem parte do domínio corporativo do IPSM, excetuando-se quando expressamente autorizados;

4 - Fazer uso de qualquer técnica forja ou simulação de falsa identidade. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme decisão do Comitê Gestor de Segurança da Informação;

5 - A interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;

6 - A utilização do serviço de comunicadores instantâneos para o envio de mensagens indesejadas (SPAM) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de comunicadores instantâneos;

7 - Usar o serviço de comunicadores instantâneos para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;

d) O usuário é o responsável exclusivo pelo uso inadequado de sua conta no serviço de comunicação instantânea, não sendo permitido o envio de mensagens cujo conteúdo incite uso de drogas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;

e) O serviço de comunicadores instantâneos é continuamente monitorado pelo IPSM, para fins de auditoria e verificação de sua devida utilização;

f) Na ocorrência de evidências de uso irregular deste serviço, o IPSM efetuará registro do incidente de segurança da informação e notificará a Autoridade Competente, que decidirá sobre o processo de abertura de sindicância administrativa, com auditoria nas contas dos usuários sob suspeita, a fim de averiguar e garantir a segurança de toda a infraestrutura de tecnologia da informação e comunicação, bem como resguardar os objetivos, com base nas legislações vigentes;

g) O monitoramento do serviço de comunicadores instantâneos do IPSM tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como cumprir à legislação em vigor;

h) Na identificação da conduta irregular por parte do usuário, será submetido à Autoridade Competente para medidas cabíveis citadas nesta Política de Segurança da Informação

i) Durante o monitoramento realizado pela ATI do IPSM, se resguarda o direito de efetuar o bloqueio da conta do Usuário, para fins de segurança.

VI - É responsabilidade da ATI - Assessoria de tecnologia da informação:

a) Controlar e monitorar os serviços de e-mail e comunicadores instantâneos fornecidos pelo IPSM;

b) Reportar ao CGSI eventuais tentativas de violação dos termos desta norma ou incidentes de segurança relacionados ao uso dos serviços de e-mail e comunicadores instantâneos.

VII - É responsabilidade do CGSI:

a) Avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria.

Art. 7º **- DA PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS - N-SI-006**

I - A Norma de segurança da informação **N-SI-006** complementa Política de Segurança da Informação, definindo as diretrizes para proteção dos ativos/serviços de informação do **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS** contra ameaças e códigos maliciosos de qualquer natureza.

II - O propósito Estabelecer diretrizes para a proteção dos ativos/serviços de informação do IPSM contra ameaças e códigos maliciosos de qualquer natureza.

III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, constante no Art. 2º desta Portaria.

IV - Ferramenta de proteção contra códigos maliciosos:

a) O IPSM disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos tais como vírus, cavalos de Tróia, vermes, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares;

b) Apenas a ferramenta disponibilizada pelo IPSM deve ser utilizada na proteção contra códigos maliciosos;

c) A ferramenta de proteção contra códigos maliciosos do IPSM adota as seguintes regras de uso:

1 - Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e varredura diária em estações de usuários e servidores corporativos;

2 - As varreduras semanais analisam todos os arquivos em cada uma das unidades de armazenamento locais das estações de usuários.

d)As varre duras diárias em servidores corporativos podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;

e) As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações;

f) Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários;

g) Caso uma estação de usuário esteja infectada ou com suspeita de infecção de código malicioso, a mesma deverá ser imediatamente isolada da rede corporativa do IPSM e de qualquer comunicação com a internet;

h) Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento do mesmo da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor;

V - Prevenção dos usuários contra códigos maliciosos:

a) Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários do IPSM devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos;

b) Os usuários do IPSM devem seguir as seguintes regras para proteção contra códigos maliciosos:

1 - Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;

2 - Reportar imediatamente a ATI qualquer infecção ou suspeita de infecção por código malicioso;

3 - Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;

4 - Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecidos pelo IPSM antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;

5 - Não habilitar MACROS para arquivos recebidos de fontes suspeitas, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio da equipe de segurança da informação para validar se o arquivo representa ou não uma ameaça.

VI - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:

a) Tratar casos de infecção ou suspeita de infecção por códigos maliciosos, reportando os mesmos a ATI, caso necessário;

b) Garantir que novas modalidades de códigos maliciosos são adequadamente investigados, tratados e protegidos pela ferramenta corporativa adotada pela IPSM;

c) Garantir a existência de iniciativas para divulgação sobre informações de ameaças, códigos maliciosos e medidas de proteção para os usuários da IPSM.

Art. 8º - **DO USO DE EQUIPAMENTOS COMPUTACIONAIS PESSOAIS - N-SI-007**

I - A Norma de segurança da informação **N-SI-007** complementa Política de Segurança da Informação, definindo as diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo do **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS** ou para o manuseio de informações do **IPSM**.

II - O propósito é estabelecer diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo do IPSM ou para o manuseio de informações do IPSM.

III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, constante no Art. 2º desta Portaria.

IV - Uso de equipamentos computacionais pessoais no ambiente corporativo:

a) Entende-se por equipamento pessoal todo o dispositivo que não foi fornecido pelo IPSM para o desenvolvimento das atividades profissionais;

b) O IPSM fornece todos os recursos computacionais necessários para que seus colaboradores executem suas atividades laborais;

c) Ao seu critério exclusivo, o IPSM poderá permitir o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade;

d) A permissão para o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade é uma prerrogativa da diretoria do IPSM, devendo o usuário estar formalmente autorizado e concordar integralmente com os termos desta norma, antes de fazer uso de dispositivos pessoais no ambiente corporativo ou para manusear informações de propriedade do IPSM;

e) O uso não autorizado de qualquer dispositivo de computação pessoal no ambiente corporativo será considerado uma violação da Política de Segurança da Informação e tratado como um incidente de segurança da informação, estando o responsável sujeito as sanções previstas nesta Política;

f) O IPSM não será responsável por guardar, fornecer suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos pessoais;

g) O uso de dispositivos de computação pessoal para atividades de trabalho ou armazenamento de arquivos do IPSM não modifica a propriedade da organização sobre as informações criadas, armazenadas, enviadas, recebidas, modificadas ou excluídas. Permanecendo qualquer direito de propriedade intelectual com o IPSM;

h) Quando autorizados a praticar o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações do IPSM, usuários serão inteiramente responsáveis por garantir a segurança de seus dispositivos, devendo garantir que:

1 - O sistema operacional dos dispositivos de computação pessoal estará sempre atualizado e com todas as correções/melhorias de segurança aplicadas;

2 - Dispositivos de computação pessoal possuem ferramenta para prevenção de códigos maliciosos e garantem que as assinaturas de códigos maliciosos são ser atualizadas em tempo real e executam varreduras diariamente;

3 - Dispositivos de computação pessoal utilizam apenas softwares licenciados, preservando o direito autoral.

i) É permitida a utilização de dispositivo pessoal e conexão à rede corporativa alternativa do IPSM, desde que haja uma solicitação da Chefia Imediata e a autorização da área responsável pela ATI;

j) O IPSM definirá os recursos ou dados corporativos disponíveis nos dispositivos particulares;

k) O IPSM não se responsabiliza pelo uso de softwares sem licenças nos dispositivos pessoais conectados à rede corporativa;

l) É de inteira responsabilidade do usuário a configuração do dispositivo pessoal conforme as regras de

segurança definidas pelo IPSM.

m) O IPSM poderá, sem aviso prévio, suspender a conexão do dispositivo pessoal com a rede corporativa em caso de suspeita de comprometimento de informações ou incidentes de segurança. Em caso de comprovação da suspeita, o acesso será revogado e as devidas providências administrativas para apuração de responsabilidade deverão ser realizadas;

n) Por se tratar de dispositivo pessoal, é de inteira e exclusiva responsabilidade do proprietário quanto a segurança dos dados nele armazenados. Deve-se utilizar mecanismos de criptografia e backup dos dados existentes, bem como o uso de softwares de antivírus e firewall;

o) Por se tratar de dispositivo pessoal, e de inteira responsabilidade do Usuário a manutenção preventiva e corretiva do equipamento, sendo vedado a solicitação de manutenção aos colaboradores da ATI.

V - É responsabilidade da ATI - Assessoria de tecnologia da informação:

a) Controlar e monitorar e autorizar o acesso a dispositivos pessoais na rede do IPSM;

b) Reportar ao CGSI eventuais tentativas de violação dos termos desta norma ou incidentes de segurança relacionados ao destes dispositivos pessoais.

VI - É responsabilidade do CGSI:

a) Avaliar, aprovar ou negar solicitações para uso de dispositivos pessoais no ambiente corporativo, bem como avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria.

Art. 9º **- DO ACESSO REMOTO - N-SI-008**

I - A Norma de segurança da informação **N-SI-008** complementa Política de Segurança da Informação, definindo as diretrizes para o acesso remoto aos ativos/serviços de informação e recursos computacionais do **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS**.

II - Estabelecer diretrizes para o acesso remoto aos ativos/serviços de informação e recursos computacionais do IPSM, garantindo níveis adequados de proteção aos mesmos.

III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, previsto ao Art. 2º desta norma.

IV - Concessão e uso do acesso remoto para Colaboradores do IPSM:

a) O acesso remoto a ativos/serviços de informação e recursos computacionais do IPSM é restrito aos usuários que necessitem deste recurso para execução das atividades profissionais;

b) O Acesso remoto será disponibilizado para os colaborares, no exercício de suas atividades relacionadas ao IPSM. O IPSM reserva para si o direito de monitorar a utilização do acesso remoto disponibilizado. A instalação e configuração ficará a cargo da ATI;

c) A ATI não se responsabiliza pelo acesso remoto, por parte do Colaborador, fora do expediente normal de trabalho;

d) O usuário será o único responsável por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por terceiros de posse de suas credencias de acesso remoto;

e) O acesso remoto aos ativos/serviços de informação e recursos computacionais do IPSM será concedido com os privilégios mínimos necessários para execução de suas atividades laborais;

f) Equipamentos computacionais utilizados para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes da IPSM e firewall local ativo;

V - O usuário, no uso do Acesso Remoto, se responsabiliza em utilizar somente seu Computador Pessoal, a fim de evitar acessos não autorizados à rede do IPSM, bem como garantir a proteção contra códigos maliciosos;

VI - Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais que possam o acesso remoto ao ambiente da IPSM habilitado, o usuário responsável deverá informar

imediatamente o ocorrido à ATI.

VII - Para criação e contas de acesso remoto, a Chefia imediata deve solicitar à ATI, por intermédio de abertura de chamado no site do IPSM, contendo os seguintes dados do Colaborador:

1 - Nome completo;

2 - Diretoria, Assessoria, Gerência ou Departamento que o Colaborador ficará alocado;

3 - Telefone/Ramal;

4 - Matricula ou Masp;

VIII - Concessão e uso do acesso remoto terceiros:

a) O acesso remoto aos ativos/serviços de informação e recursos computacionais do IPSM poderá ser concedido pela ATI a terceiros ou prestadores de serviço, caso seja necessário para suas atividades laborais;

b) Para concessão e uso do acesso remoto para terceiros, devem ser observadas as seguintes regras:

1 - O acesso remoto de terceiros e prestadores de serviço aos ativos/serviços de informação ou recursos computacionais do IPSM somente poderá ser concedido após a efetivação e assinatura da Política de Segurança da Informação e a assinatura do acordo de confidencialidade entre as partes;

2 - A concessão do acesso deverá ser limitada automaticamente ao tempo necessário estimado a atividade do terceiro ou prestador de serviço;

3 - O usuário terceiro, bem como a empresa onde o mesmo trabalha, serão os únicos responsáveis por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por outras partes de posse de suas credencias de acesso remoto;

c) O acesso remoto de terceiros aos ativos/serviços de informação e recursos computacionais do IPSM será concedido com os privilégios mínimos necessários para execução de suas atividades laborais;

d) Equipamentos computacionais utilizados por terceiros para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes da IPSM e firewall local ativo;

e) O usuário terceiro, no uso do Acesso Remoto, se responsabiliza em utilizar somente seu Computador Corporativo, a fim de evitar acessos não autorizados à rede do IPSM, bem como garantir a proteção contra códigos maliciosos;

f) Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais de terceiros que possam o acesso remoto ao ambiente da IPSM habilitado, o usuário responsável deverá informar imediatamente o ocorrido a ATI;

g) Toda informação que é acessada, transmitida, recebida ou produzida através do acesso remoto aos ativos/serviços de informação ou recursos computacionais do IPSM é continuamente monitorado pelo IPSM;

h) Na ocorrência de evidências de uso irregular deste serviço, o IPSM efetuará registro do incidente de segurança da informação e notificará a Autoridade Competente, que decidirá sobre o processo de abertura de sindicância administrativa, com auditoria nas contas do Usuário sob suspeita, a fim de averiguar e garantir a segurança de toda a infraestrutura de tecnologia da informação e comunicação, bem como resguardar os objetivos com base nas legislações vigentes;

i) Durante o monitoramento do acesso remoto aos seus ativos/serviços de informação ou recursos computacionais, o IPSM se resguarda o direito de notificar ou avisar o usuário;

j) Na identificação da conduta irregular por parte do usuário, será submetido à Autoridade Competente para medidas cabíveis citadas nesta Política de Segurança da Informação;

k) Durante o monitoramento realizado pela ATI do IPSM, se resguarda o direito de efetuar o bloqueio da conta do Usuário, para fins de segurança;

IX - Para criação e contas de acesso remoto a pessoal externo ao IPSM, a Chefia imediata deve solicitar a ATI, por intermédio de abertura de chamado no Site do IPSM, contendo os seguintes dados do Colaborador:

1 - Nome completo;

2 - Justificativa pelo acesso remoto e o período a ser concedido;

3 - Diretoria, Assessoria, Gerência ou Departamento que o Colaborador que estará atuando;

4 - Telefone pessoal ou Corporativo;

X - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:

a) Avaliar, aprovar ou negar solicitações para uso de acesso remoto a ativos/serviços de informação ou recursos computacionais do IPSM**;**

b) Controlar e monitorar qualquer tipo de acesso remoto fornecido pelo IPSM;

c) Tratar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso remoto e, quando pertinente, reportar os mesmos ao CGSI.

XI - É responsabilidade do CGSI:

a) Avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria.

Art. 10 º **- DO MONITORAMENTO DE ATIVOS E SERVIÇOS DA INFORMAÇÃO - N-SI-009**

I - A Norma de segurança da informação **N-SI-009** complementa Política de Segurança da Informação, definindo as diretrizes para o monitoramento de ativos/serviços de informação e recursos computacionais do **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS**.

II - O propósito é estabelecer diretrizes para o monitoramento de ativos/serviços de informação e recursos computacionais do IPSM, garantindo o respeito dos usuários às regras estabelecidas na Política de Segurança da Informação, bem como produzir prova de eventual violação das condições constantes da mesma, e na legislação vigente.

III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, contida no Art. 2º desta Portaria..

IV - Monitoramento de ativos/serviços da informação e recursos computacionais:

a) Qualquer ativo/serviço de informação ou recurso computacional do IPSM, bem como qualquer outro recurso computacional com acesso aos mesmos, poderá ser monitorado a qualquer momento;

b) Todos os ativos/serviços de informação, recursos computacionais do IPSM, bem como toda informação trafegada ou armazenada nos mesmos, incluindo conta de e-mail corporativa e a navegação em sites e serviços da Internet são monitorados pelo IPSM;

c) O IPSM se resguarda o direito de notificar ou avisar o usuário sobre as ilegalidades a serem ocorridas, onde haverá bloqueio da conta do Usuário, que após procedimento administrativo, o IPSM poderá verificar o conteúdo da Conta;

d) Na utilização dos ativos/serviços de informação ou recursos computacionais do IPSM, incluindo a utilização da conta de e-mail corporativa, comunicadores instantâneos e navegação em sites da Internet, através da infraestrutura tecnológica do IPSM, o monitoramento tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como cumprir à legislação em vigor;

e) Durante o monitoramento dos serviços, o IPSM se resguarda o direito de notificar ou avisar o usuário sobre as ilegalidades a serem ocorridas nos ativos/serviços de informação ou recursos computacionais do IPSM, onde haverá bloqueio da conta do Usuário;

f) O IPSM efetuará registro do incidente de segurança da informação e notificará a Autoridade Competente, que decidirá sobre o processo de abertura de sindicância administrativa, com auditoria nas contas do Usuário sob suspeita, a fim de averiguar e garantir a segurança de toda a infraestrutura de tecnologia da informação e comunicação, bem como resguardar os objetivos com base nas legislações vigentes;

g) Durante o monitoramento dos ativos/serviços de informação ou recursos computacionais, o IPSM se resguarda o direito de notificar ou avisar o usuário;

h) Na identificação da conduta irregular por parte do usuário, será submetido à Autoridade Competente para medidas cabíveis citadas nesta Política de Segurança da Informação;

i) Durante o monitoramento realizado pela ATI do IPSM, se resguarda o direito de efetuar o bloqueio da conta do Usuário, para fins de segurança.

V - Do aviso legal:

a) O IPSM faz uso de um aviso legal para garantir que usuários e demais pessoas e entidades que tentem obter acesso aos ativos/serviços de informação ou recursos computacionais da organização estejam cientes das regras de segurança adotadas pelo IPSM, bem como do monitoramento realizado nos termos desta norma;

b) O aviso legal deverá ser exibido antes de permitir o acesso aos ativos/serviços de informação ou recursos computacionais do IPSM, apresentando o seguinte formato:

- "Este é um ativo/serviço de informação ou recurso computacional do IPSM, o qual pode ser acessado e utilizado somente por usuários previamente autorizados. Em caso de acesso e uso não autorizado ou indevido deste sistema, o usuário estará sujeito sanções cabíveis nas legislações aplicáveis. Este ativo/serviço de informação ou recurso computacional é monitorado. O acesso a este ativo/serviço de informação ou recurso computacional ou o uso do mesmo por qualquer pessoa ou entidade, autorizada ou não, constitui seu consentimento irrestrito aos termos aqui expostos."

c) O acesso a qualquer ativo/serviço de informação ou recurso computacional do IPSM ou o uso dos mesmos por qualquer pessoa ou entidade, autorizada ou não, caracteriza consentimento irrestrito aos termos expostos no aviso legal;

d) A ausência do aviso legal em qualquer ativo/serviço de informação ou recurso computacional do IPSM não descaracteriza a necessidade de cumprimento das regras expostas nas políticas, normas e demais procedimentos de segurança da informação adotados pelo IPSM.

VI - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:

a) Realizar o monitoramento dos ativos/serviços de informação ou recursos computacionais do IPSM;

b) Tratar eventuais violações das diretrizes de segurança do IPSM identificadas através de ferramentas de monitoramento, e, quando pertinente, reportar as mesmas ao CGSI.

VII - É responsabilidade do CGSI:

a) Avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria.

Art. 11º - **DA RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO - N-SI-010**

I - A Norma de segurança da informação **N-SI-010** complementa Política de Segurança da Informação, definindo as diretrizes para responder eventos ou incidentes de segurança estejam impactando ou possam vir a impactar ativos/serviços de informação ou recursos computacionais do **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS.**

II - O propósito é estabelecer diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informação que possam impactar ativos/serviços de informação ou recursos computacionais do IPSM.

III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, constante no Art. 2º da Portaria.

IV - Incidentes de segurança da informação:

a) Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais do IPSM serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados;

b) Incidentes de segurança devem ser priorizados com base na criticidade dos ativos/serviços de

informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista;

c) Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados a ATI;

d) A ATI deverá determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas;

e) Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente;

f) A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados;

g) Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

V - Time de resposta a incidentes de segurança da informação:

a) O time de resposta a incidentes de segurança da informação do IPSM deverá ser composto por, no mínimo, representantes das seguintes áreas:

1 - Assessoria de Tecnologia da Informação;

2 - Comitê Gestor de Segurança Da Informação

3 - Procuradoria.

b) Conforme a natureza do incidente, colaboradores de qualquer setor do IPSM podem ser convocados a participar do time de resposta a incidentes de segurança da informação;

c) O time de segurança da informação será concebido nos casos reais de violação de segurança, ficando a cargo do CGSI em conjunto com a Diretoria do IPSM a designação de seus integrantes.

VI - Disseminação de informação sobre incidentes de segurança da informação:

a) Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas ao IPSM sem aprovação expressa e formal da diretoria.

VII - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:

a) Atuar como responsável por ocorrências e eventos de segurança e garantir a existência de recursos, identificar, escalar, mitigar, conter, e erradicar incidentes de segurança, bem como ações efetivas para recuperar o estado anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente.

b) Comunicar prontamente o time de resposta a incidentes de segurança da informação do IPSM, caso houver, sobre eventos e incidentes de segurança.

c) Apoiar no tratamento de ocorrências e incidentes de segurança da informação, fornecendo orientação e direcionamento estratégico dentro da área de especialidade de cada um dos participantes do time de resposta aos incidentes de segurança da informação;

d) Aconselhar a diretoria do IPSM sobre quais informações sobre eventos e incidentes de segurança da informação podem ser divulgadas para públicos internos e externos.

VIII - É responsabilidade da Procuradoria:

a) No que couber, apoiar nas respostas administrativas e atuações judiciais necessárias conforme identificação da ocorrência.

IX - É responsabilidade do CGSI:

a) Apoiar na identificação dos possíveis vazamentos e no plano de respostas ao incidente;

b) Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público;

c) Elenca, em conjunto com a Diretoria do IPSM, nos termos do Inciso V deste Artigo, servidores para analisar as violações de segurança, ocorridas no IPSM, nos temos desta Política de Segurança da Informação, bem como auxiliar a Diretoria na elaboração da resposta ao incidente.

Art. 12º - Sanções serão avaliadas conforme previsto na Política de Segurança da Informação e normas complementares, e que serão submetidos à Autoridade Competente para medidas cabíveis citadas na mesma.

Art. 13º - Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

Art. 14º - A Portaria é aprovada pela Diretoria do **IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS**.

Art. 15º - Esta Portaria entra em vigor na data de sua publicação.

Belo Horizonte, 11 de agosto de 2023.

Fabiano Villas Boas, Cel. PM QOR

Diretor-Geral do IPSM

Documento assinado eletronicamente por **Fabiano Villas Boas**, **Diretor(a) Geral**, em 11/08/2023, às 15:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **70985592** e o código CRC **70819E36**.

Referência: Processo nº 2120.01.0008850/2022-40 SEI nº 70985592

MINAS GERAIS

WWW.JORNALMINASGERAIS.MG.GOV.BR ANO 131 – Nº 162 – 91 PÁGINAS BELO HORIZONTE, QUINTA-FEIRA, 17 DE AGOSTO DE 2023

Instituto de Previdência dos Servidores Militares - IPSM

Cel PM QOR Fabiano Villas Boas

PORTARIA DG Nº 1124/2023

Institui a Política de Segurança da Informação - PSI , no âmbito do Instituto de Previdência dos Servidores Militares - IPSM.

O Diretor-Geral do Instituto de Previdência dos Servidores Militares do Estado de Minas Gerais (IPSM), no uso das atribuições que lhe confere art. 7º, inciso I, do Decreto 48.064, de 16 de outubro de 2020,

RESOLVE:

Art. 1º - Instituir a Política de Segurança da Informação - PSI no âmbito do IPSM, conforme normas nesta Portaria.

Art. 2º - DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI-001

I - O IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DE MINAS GERAIS tem como missão, garantir o benefício previdenciário e promover a atenção à saúde por meio de ações administrativas, em prol da segurança e qualidade de vida da Família Militar Mineira. Tem como visão, ser reconhecido como Entidade de excelência na gestão do Regime Próprio de Previdência dos militares do Estado e na promoção da assistência à saúde. Tem como princípios e valores da Confidencialidade, Integridade, Disponibilidade, Autenticidade, Legalidade, Finalidade, Adequação, Necessidade, Livre acesso, Qualidade dos dados, Transparência, Segurança, Prevenção, Não discriminação, Responsabilização e prestação de contas.

II - Esta Política de Segurança da Informação do IPSM tem respaldo legal nas legislações a seguir: Lei Federal nº 12.965/2014, Lei Federal nº 12.527/2011, Lei Federal nº 13.460/2017, Lei Federal nº 13.709/2018, Decreto Estadual nº 47.974/2020, Decreto Estadual nº 45.969/2022, Decreto Estadual nº 46.226/2013, Decreto Estadual nº 45.241/2009, Decreto Estadual nº 48.383/2022, Resolução SEPLAG Nº 084/ 2022.

III - Em casos omissos, deverá ser observado a Resolução SEPLAG nº 084, DE 11 de novembro de 2022 e legislações da Tecnologia da Informação vigente, do Estado de Minas Gerais.

IV - O IPSM entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados aos seus beneficiários.

V - O IPSM compreende que as manipulações das informações passam por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

VII - Dessa forma, o IPSM estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção às informações da organização ou sob sua responsabilidade, em conformidade com a Resolução SEPLAG nº 084/2022.

VIII - Para os fins desta Portaria, considera-se:

a) IPSM: Instituto de Previdência dos Servidores Militares do Estado de Minas Gerais;

b) ATI: Assessoria de Tecnologia da Informação;

c) GRH: Gerência de Recursos Humanos;

d) DRH: Departamento de Recursos Humanos;

e) DLT: Departamento de Logística e Transporte;

f) Ameaça: causa potencial de um incidente, que pode vir a prejudicar o IPSM;

g) Ativo: tudo aquilo que possui valor para o IPSM;

h) Ativo de informação: patrimônio intangível do IPSM, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas ao IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS por parceiros, beneficiários, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional do IPSM ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídias eletrônicas transitadas dentro e fora de sua estrutura física;

i) Comitê Gestor de Segurança Da Informação – CGSI: grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do IPSM, que tem por finalidade tratar questões ligadas à Segurança da Informação;

j) Confidencialidade: propriedade dos ativos da informação do IPSM, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas;

k) Controle: medida de segurança adotada pelo IPSM para o tratamento de um risco específico;

l) Disponibilidade: propriedade dos ativos da informação do IPSM, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas;

m) Gestor da Informação: usuário da informação que ocupe cargo especifico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação;

n) Incidente de segurança da informação: um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações do IPSM;

o) Integridade: propriedade dos ativos da informação do IPSM, de serem exatos e completos;

p) Risco de segurança da informação: efeito da incerteza sobre os objetivos de segurança da informação do IPSM;

q) Segurança da informação: a preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do IPSM;

r) Usuário da informação: empregados com vínculo empregatício de qualquer área do IPSM ou terceiros alocados na prestação de serviços o IPSM, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação do IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DE MINAS GERAIS para o desempenho de suas atividades profissionais;

s) Vulnerabilidade: causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações do IPSM.

IX - Esta política como propósito:

a) Estabelecer diretrizes e normas de Segurança da Informação que permitam aos servidores, colaboradores, beneficiários e a todos que utilizam dos serviços prestados pelo IPSM adotarem padrões de comportamento seguro, adequados às metas e necessidades do IPSM, aplicando também a fornecedores no desempenho de alguma atividade internamente ao ambiente lógico do IPSM;

b) Orientar quanto à adoção de controles e processos para atendimentodos requisitos para Segurança da Informação;

c) Resguardar as informações do IPSM, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

d) Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus servidores, colaboradores, beneficiários e parceiros;

e) Minimizar os riscos de perda, da confiança de beneficiários ou qualquer outro impacto negativo nos serviços prestados pelo IPSM como resultado de falhas de segurança da informação.

X - Esta política se aplica a todos os usuários da informação do IPSM, incluindo qualquer indivíduo ou organização que possui ou possuiu vinculo com o IPSM, tais como servidores ativos e aposentados, estagiários, beneficiários, empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuem ou virão a possuir acesso às informações do IPSM e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura do IPSM.

XI - O objetivo da Gestão de Segurança da Informação do IPSM é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactosa instituição.

XII - A Diretoria do IPSM e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação no IPSM. Desta forma, adotam todas as medidas cabíveispara garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades do IPSM.

XIII - É política do IPSM:

a) Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação do IPSM sejam atingidos através da adoção de controlescontra ameaças provenientes de fontes tanto externas quanto internas;

b) Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: servidores, colaboradores, empregados, beneficiários, terceiros contratados e, ondefor pertinente;

c) Garantir a educação e conscientização sobre as práticas adotadas pelo IPSM de segurança da informação para servidores, colaboradores, terceiros contratados e, onde for pertinente, beneficiários;

d) Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

e) Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e , quando necessário, comunicando as autoridades apropriadas;

f) Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

g) Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança emtodos os níveis da organização.

XIV - Do Comitê Gestor de Segurança da Informação – CGSI:

a) Fica constituído o COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO, contando com a participação de, pelo menos, um representante da diretoria e um membro sênior das seguintes áreas: ATI - Assessoria de Tecnologia da Informação, Gerência de Recursos Humanos, Procuradoria e Representante da Previdência e Saúde.

b) É responsabilidade do CGSI:

1) Analisar, revisar e propor a aprovação de políticas e normas e diretrizes relacionadas à segurança da informação;

2) Garantir a disponibilidade dos recursos necessários para uma efetivaGestão de Segurança da Informação;

3) Garantir que as atividades de segurança da informação sejam executadas em conformidade com a Política de Segurança da Informação do IPSM e seus anexos;

4) Promover a divulgação da PSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do IPSM;

5) Avaliar irregularidades reportadas pela ATI e, havendo necessidade,reportar à Diretoria;

6) Avaliar, aprovar ou negar solicitações para uso de dispositivos pessoais no ambiente corporativo, bem como avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria;

7) Elencar, em conjunto coma a Diretoria do IPSM, nos termos da Política de Segurança da Informação, servidores para analisar as violações de segurança, ocorridas no IPSM, bem como auxiliar a Diretoria na elaboração da resposta ao incidente.

XV - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:

a) Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CGSI;

b) Apoiar o CGSI em suas deliberações;

c) Elaborar e propor ao CGSI as normas e procedimentos de segurançada informação, necessários para se fazer cumprir a PSI;

d) Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

e) Tomar as ações cabíveis para se fazer cumprir os termos desta política;

f) Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado;

g) Manter os sistemas computacionais e de comunicação em conformidade com a Política de Segurança da Informação;

h) Disponibilizar os recursos necessários à implantação da Política de Segurança da Informação;

i) Manter os dados cadastrais dos usuários da rede corporativa, bem como do correio eletrônico, atualizados;

j) Reportar incidentes de segurança da informação à área responsável;

k) Monitorar os logs dos sistemas;

l) Acompanhar a realização de manutenção, corretiva ou preventiva, dos servidores e subsistemas de armazenamento da rede corporativa do IPSM quando a manutenção for realizada por terceiros no ambientedo IPSM;

m) Prestar suporte ao usuário quando solicitado;

n) Solicitar apoio e consultoria de segurança à área responsável pela Segurança da Informação quando se fizer necessário, caso houver;

o) Solicitar a assinatura do Termo de Confidencialidade do usuário;

p) Instalar e configurar os Computadores nas estações de trabalho;

q) Manter um inventário atualizado dos computadores e dos softwares;

r) Desenvolver e manter um padrão de instalação e configuração dos computadores, aderente aos critérios estabelecidos pelo IPSM;

s) Configurar os programas de computador e equipamentos para garantira utilização dos critérios relativos às senhas de acesso definidos;

t) Manter o antivírus, anti-spam e as correções de segurança dos servidores e computadores atualizados;

u) Lacrar os computadores;

v) Disponibilizar e administrar a infraestrutura necessária para armazenamento de dados;

w) Disponibilizar e administrar os recursos de acesso à Internet;

x) Monitorar o uso da Internet;

y) Registrar os acessos indevidos à Internet;

z) Orientar os usuários em relação à proteção adequada dos dispositivos móveis;
aa) Configurar os dispositivos móveis disponibilizados para os usuários do IPSM;
bb) Instalar, homologar, manter, atualizar e configurar todos os servidores, subsistemas de armazenamento e programas de computador que componham as soluções de backup e restore utilizadas no IPSM;
cc) Manter a documentação dos servidores, subsistemas de armazenamento, e programas de computador diretamente vinculados às soluções de backup e restore;
dd) Realizar o backup e a remoção das informações armazenadas nos servidores e subsistemas de armazenamento da rede corporativa do IPSM, no caso de manutenção externa ao IPSM;
ee) Definir os recursos e ferramentas que serão utilizados em cada procedimento de backup e restore;
ff) Documentar os procedimentos de backup e restore;
gg) Eliminar e substituir as mídias de backup e restore próximas de perderem sua funcionalidade segundo a vida útil informada pelo fornecedor;
hh) Eliminar o conteúdo das mídias que serão descartadas;
ii) Executar os procedimentos de backup e restore;
jj) Gerenciar e controlar os recursos computacionais e as mídias utilizadas pelos sistemas de backup e restore do IPSM;
kk) Manter mapa atualizado das mídias e seus conteúdos para todos os procedimentos de backup e restore do IPSM;
ll) Planejar junto às áreas solicitantes os procedimentos de backup e restore;
mm) Realizar testes de validação e desempenho das cópias de segurança realizadas;
nn) Disponibilizar os recursos necessários para a execução das funções de auditoria;
oo) Garantir a proteção adequada das trilhas de auditoria;
pp) Aprovar e registrar a utilização das ferramentas de monitoramento e acesso às estações de trabalho;
qq) Analisar e despachar os expedientes relativos a solicitações de usuários encaminhadas pelos respectivos responsáveis por suas unidades;
rr) Administrar o acesso remoto à rede do IPSM;
ss) Definir os softwares autorizados que deverão ser instalados nas estações de trabalho;
tt) Administrar as redes corporativas do IPSM;
uu) Manter a documentação da topologia da rede atualizada e controlar o acesso ao seu conteúdo;
vv) Prover o ambiente físico necessário para instalação dos roteadores e switches;
ww) homologar e administrar os roteadores e switches do IPSM;
xx) Manter a documentação (topologia, configurações, etc) dos roteadores e switches atualizada;
yy) Administrar as regras dos firewalls;
zz) Instalar, configurar e manter os ambientes operacionais dos firewalls - sistema operacional nos servidores, bem como os produtos e as correções e atualizações de versão;
aaa) Aplicar, anualmente, os controles disponibilizados pela ferramenta de gestão de riscos nos ativos em que estejam instalados os firewalls;
bbb) Manter atualizadas as documentações (configurações) relativas aos firewalls;
ccc) Disponibilizar a infraestrutura necessária para o funcionamento da solução de network IDS/IPS;
ddd) Instalar e administrar o network IDS/IPS;
eee) Analisar periodicamente as logs dos Networks IDS em busca de incidentes de Segurança da Informação;
fff) Avaliar, o desempenho do network IDS/IPS em relação à quantidade de ataques detectados, falsos positivos (alarme falso), carga da rede, entre outros;
ggg) Manter a documentação do network IDS/IPS atualizada;
hhh) Instalar, homologar, manter e configurar todos os equipamentos de conectividade que componham as soluções de backup e restore utilizadas no IPSM;
iii) Definir e implementar rotina automatizada para a cópia das configurações e dados dos equipamentos de conectividade para um servidor de arquivos contemplado por uma das rotinas de backup/restore;
jjj) Analisar e emitir parecer sobre as solicitações da área de segurança da informação, quando houver e se solicitado;
kkk) Atualizar os controles da ferramenta de análise de risco de Segurança da Informação, caso houver;
lll) Avaliar e aplicar, para as situações consideradas críticas, os controles existentes na ferramenta de análise de risco de Segurança da Informação;
mmm) Elaborar e manter atualizado um procedimento de instalação e configuração da rede;
nnn) Administrar a cessão, a alteração, o bloqueio e o cancelamento de acessos à rede corporativa;
ooo) Revisar os direitos de acesso dos usuários da rede corporativa e realizar as alterações necessárias;
ppp) Revisar, os direitos de acesso com privilégios de administrador e realizar as alterações necessárias;
qqq) Definir, homologar, implementar e disponibilizar a infraestrutura e os mecanismos de segurança para utilização da rede wireless;
rrr) Realizar análise de risco na rede wireless;
sss) Disponibilizar relatório as conexões remotas realizadas;
ttt) Solicitar a autorização para movimentação patrimonial de ativos (hardware) ao DLT.
XVI - É responsabilidade dos Gestores da Informação:
a) Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo IPSM;
b) Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pelo IPSM;
c) Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;
d) Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;
e) Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo IPSM.
XVII - É responsabilidade dos Usuários da Informação:
a) Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
b) Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, suas normas e procedimentosa ATI ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;
c) Comunicar à ATI qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais do IPSM;
d) Assinar o Termo de Uso de Sistemas de Informação do IPSM, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;
e) Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções;
f) Sugerir medidas que possam elevar os níveis de segurança das instalações na sua área de atuação;
g) Responder pelo uso de seu login de acesso aos sistemas e serviços do IPSM;
h) Zelar pelas informações, sistemas, serviços e recursos de tecnologia da informação sob sua responsabilidade;
i) Não realizar alterações na configuração do computador sem autorização;
j) Utilizar adequadamente os recursos computacionais;
k) Conduzir adequadamente o uso da Internet, respeitando direitos autorais, regras de licenciamento de softwares, direitos de propriedade e privacidade;
l) Alterar a senha no momento em que receber as informações da criação de sua conta;
m) Manter sigilo de seu login e de sua senha de acesso aos sistemas e serviços do órgão ou entidade;
n) Trocar a senha sempre que houver indícios de comprometimento do sistema ou da própria senha;
o) Guardar as mídias removíveis, contendo dados, em armários com chaves;
p) Eliminar os arquivos desnecessários armazenados nos servidores da rede do IPSM;
q) Responder pelo uso de dispositivos particulares no ambiente do IPSM;
r) Solicitar à Chefia imediata a utilização e a conexão do dispositivo móvel na rede corporativa justificando a sua necessidade;
s) Evitar armazenar informações confidenciais em dispositivosmóveis usados fora do órgão ou entidade. Havendo necessidade, tais informações deverão ser transferidas para um local de armazenamento seguro logo que possível;
t) Ser responsável pelos dispositivos móveis, e pelos dados armazenados nos mesmos, disponibilizados para uso dentro e fora das instalações do IPSM;
u) Não deixar os dispositivos móveis desprotegidos em locais dealto risco, tais como locais públicos, eventos, hotéis, veículos, dentre outros;
v) Apresentar em caso de furto, roubo ou extravio do dispositivo móvel a Ocorrência Policial, no prazo máximo de 48 horas do fato ocorrido, à área responsável pelo patrimônio do IPSM;
w) Apresentar o dispositivo móvel para a área responsável pelo atendimento ao usuário, quando requisitado, ou ao cessar as atividades que motivaram sua solicitação;
x) Zelar pela guarda do dispositivo de armazenamento do certificado digital e pela senha de acesso ao dispositivo;
y) Requisitar a revogação do certificado digital caso ele seja perdido, roubado ou extraviado, informando imediatamente o fato à área responsável;
XVII - O usuário que não cumprir as normas estabelecidas nessa Política estará sujeito às penalidades previstas em Lei.
XVIII - Será avaliado pelo Comitê Gestor de Segurança da Informação - CGSI do IPSM, a ser criado por Portaria interna do Diretor-Geral do IPSM, onde o CGSI, informará autoridade competente, que verificará a gravidade dos fatos, e, nos casos de servidores podendo gerar um processo interno para avaliação.
XIX - O descumprimento do disposto nesta Política sujeitará o servidor, o prestador de serviço terceirizado e o estagiário às sanções e às penalidades previstas em lei, assegurados o contraditório e a ampla defesa.
XX - Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano o IPSM ou a outrem, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes pelos Órgãos Competentes, sem prejuízo aos termos descritos nesta política.
XXI - Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.
XXII - As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança constantes a seguir nesta Portaria, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças.
XXIII - Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do IPSM adotar, sempre que possível outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações do IPSM.
XIV - As normas a seguir complementam a Política de Segurança da informação - PSI do IPSM.
Art. 3º - DA NORMA DE USO ACEITÁVEL DE ATIVOS DE INFORMAÇÃO - N-SI-002
I - A Norma de segurança da informação N-SI-002 complementa Política de Segurança da Informação, definindo as diretrizes para o uso aceitável de ativos de informação do IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS por seus usuários autorizados.
II - Seu propósito é estabelecer diretrizes para o uso aceitável, entendido como seguro, dos ativos de informação do IPSM por seus usuários autorizados.
III Esta norma obedece ao escopo definido na Política de Segurança da Informação, constante no Art. 2º desta Portaria.
IV - Uso de equipamento computacional:
a) O IPSM fornece para seus usuários equipamentos para o desempenho exclusivamente de suas atividades profissionais;
b) Todo usuário deve observar as seguintes disposições quanto ao uso de equipamentos de propriedade do IPSM;
c) Os equipamentos disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais são de propriedade do IPSM, sendo expressamente proibida a utilização para fins particulares;
d) A alteração e/ou a manutenção de qualquer equipamento de propriedade do IPSM é uma atribuição específica da ATI que, ao seu critério exclusivo, poderá delegar formalmente outro responsável. Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos;
e) Os equipamentos do IPSM devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado;
f) Computadores de mesa (desktops) ou móveis (notebooks) e (tablet) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado, exceto quando existir uma justificativa plausível em virtude de atividades de trabalho;
g) A desconexão (log off) da rede deverá ser efetuada nos casos em que o usuário não for mais utilizar o equipamento ou venha a ausentar-se por um período prolongado;
h) O bloqueio de tela protegido por senha deverá ser ativado sempre que o usuário se afastar do computador de mesa ou móvel que esteja utilizando;
i) Os equipamentos disponibilizados pelo IPSM, para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado e original quando no desligamento ou término da relação do usuário com do IPSM, sendo que para equipamentos considerados permanentes, a chefia imediata deve solicitar sua devolução, para retirada do material do mapa carga junto ao DLT;
j) O DLT solicitará a ATI a avaliação de equipamentos informacionais para finalização da Baixa de carga patrimonial. Constatado qualquer dano aos equipamentos do IPSM será devidamente analisado pela ATI. Havendo a constatação de que tal dano decorreu de mau uso do usuário, caberá a IPSM exercer seu direito de reparação ao prejuízo, através da tomada das medidas administrativas cabíveis;
h) Para avaliação do material, o usuário deverá realizar abertura do Chamado no site do IPSM, para avaliação do material pela ATI. Será realizado agendamento de data e hora. Será elaborado parecer técnico (laudo do material) pela área responsável do IPSM onde constará o estado do material. A ATI enviará o laudo para o DLT para demais providências cabíveis;
i) Caso seja detectado mau uso ou avariais no equipamento, o usuário será notificado para maiores explicações;
j) Caso o equipamento com avariais ou defeito esteja impossibilitado para uso, o DLT solicitará à ATI uma avaliação mais minuciosa do defeito e em casos específicos de defeitos do hardware, será enviado para uma assistência técnica especializada para emissão de um relatório circunstanciado sobre o defeito do equipamento;
k) Comprovado o mau uso do equipamento, o DLT acionará o usuário e o mesmo poderá:
1 - Procurar um técnico de sua confiança para realização do conserto, por sua conta e risco, sendo que o equipamento após o conserto passará por nova avaliação do DLT e da ATI, com emissão de novo laudo;
2 - Caso em que o usuário não opte pelo conserto, ele terá a opção de realizar a compra de um material igual ou superior, com as mesmas características técnicas, equivalente, capaz de atender às suas necessidades de forma satisfatória o IPSM. O aparelho deve ser novo, sem uso e deverá passar por nova emissão de avaliação técnica do IPSM;
3 - Autorizado pelo Usuário, o IPSM solicitará o conserto do notebook sendo que os custos do conserto e troca de peças ficará a cargo do usuário que casou dano ao material.
l) Em caso de perda ou furto de equipamento de propriedade do IPSM, o usuário deverá comunicar imediatamente o DLT e a ATI para que possam ser tomadas as medidas cabíveis de revogação de acessos a rede do IPSM bem como de outros sistemas que o Usuário possua e ainda deverá realizar boletim de ocorrência apresentando o respectivo documento no momento da comunicação ao DLT/ATI;
j) A seu critério exclusivo o IPSM poderá permitir a utilização de equipamento particular para o desempenho de atividades profissionais, devendo os mesmos passar por inspeção da ATI de forma a garantir adequação aos requisitos e controles de segurança adotados pela empresa;
k) Não é permitida a conexão de equipamentos particulares na rede administrativa do IPSM, seja em segmentos cabeados ou sem fio, sem autorização prévia formal e inspeção do equipamento pela ATI;
V - Dispositivos de Armazenamento Removível:
a) O IPSM poderá, ao seu critério exclusivo, fornecer aos seus usuários dispositivos móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, devendo ser observadas além das diretrizes acima, as seguintes;
b) O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda;
c) O dispositivo será de uso e responsabilidade de seu usuário, nos termos do formulário de recebimento do DLT (Termo de Cessão de Uso), assinado no momento de entrega;
d) O Usuário, na utilização dos dispositivos móveis fora do ambiente do IPSM, deverá estar alerta e ter uma conduta discreta e zelando pela material, dando preferência para compartimentos de armazenamento resistentes;
e) A instalação de ferramentas de proteção para dispositivos móveis é realizada exclusivamente pela ATI e é obrigatória para todos os equipamentos corporativos; e
f) Em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deverá comunicar imediatamente o DLT e a ATI para que possam ser tomadas as medidas cabíveis e deverá realizar boletim de ocorrência apresentando o respectivo documento no momento da comunicação ao DLT.
VI - Identificação digital:
a) O IPSM poderá, ao seu critério exclusivo ou conforme legislação pertinente, fornecer certificados digitais para usuários que execução de atividades profissionais específicas, devendo ser observadas as seguintes diretrizes;
b) Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo;
c) O usuário deverá informar a ATI sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;
d) O usuário desligado ou em processo de desligamento terá o certificado digital expedido pelo IPSM imediatamente revogado;
f) É de responsabilidade da ATI prover a atualização de todos os pontos de verificação com as respectivas listas de revogação.
VII - Equipamentos de impressão e reprografia:
a) O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse do IPSM ou que estejam relacionados com o desempenho das atividades profissionais do usuário;
b) O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de impressão e reprografia;
c) O usuário deve retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações do IPSM, classificadas como de uso interno ou confidencial;
d) A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;
e) Não será admissível, o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais ou pessoais, devendo as mesmas ser descartadas de acordo com os procedimentos adotados pelo IPSM.
VIII - Segurança física dos ativos de informação:
a) As instalações de processamento das informações do IPSM serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, ou os danos e quaisquer interferências de origem humana ou natural;
b) Deverá ser observado as seguintes disposições específicas quanto à segurança física;
c) Crachás de identificação de terceiros e autorizado, inclusive temporários expedidos pelo IPSM, são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;
d) Estando em áreas sensíveis, os colaboradores devem portar crachás de identificação que exibam claramente seu nome e fotografia. Terceiros autorizados devem portar crachás temporários pelo IPSM identificando claramente que os mesmos não são colaboradores;
e) Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;
f) É proibida qualquer tentativa de se obter ou permitir o acesso aos indivíduos não autorizado a áreas sensíveis do IPSM;
g) É resguardado ao IPSM o direito de monitorar seus ambientes físicos. Para isso será utilizado sistema de circuito fechado de televisão em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida, e serão utilizadas exclusivamente para verificação interna, não podendo ser solicitada para outro fim, exceto em casos previstos em lei;
h) Não é permitido consumir qualquer tipo de alimento, bebida ou fumar em áreas apontadas como sensíveis, incluindo computadores e seus periféricos, bem como quaisquer dispositivos móveis de responsabilidade do IPSM.
IX - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:
a) Estabelecer e manter atualizados os procedimentos complementares a esta norma;
b) Comunicar ao CGSI eventuais tentativas, bem sucedidas ou não, de desvio de conduta dos termos dessa norma.
Art. 4º - GESTÃO DE IDENTIDADE DE CONTROLE DE ACESSO - N-SI-003
I - A Norma de segurança da informação N-SI-003 complementa Política de Segurança da Informação, definindo as diretrizes para garantir que o acesso aos ativos de informação ou sistemas de informação do IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS garanta níveis adequados de proteção.
II - Seu propósito é estabelecer diretrizes para gestão de identidade e acesso aos ativos e sistemas de informação do IPSM.
III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, constante no Art. 2º desta Portaria.
IV - Acesso a ativos e sistemas de informação:
a) O IPSM fornece aos seus usuários autorizados contas de acesso aos sistemas cadastrados que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa;
b) As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;
c) Toda conta de acesso é pessoal do usuário a qual foi delegada e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso.
d) Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro aos ativos e serviços de informação, incluindo:
1 - Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pelo IPSM;
2 - Não utilizar sua conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pelo IPSM;
3 - Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;
4 - Informar imediatamente a ATI caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais do IPSM.
e) Usuários que tem acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica fornecida pelo IPSM que pode ser um cartão de acesso, biometria ou uma conta de criada para acesso aos sistemas – com privilégios administrativos, para este propósito. A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia;
f) Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviçosde informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração e notificação pela Autoridade Competente que analisará a aplicação das sanções previstas na Política de Segurança da Informação, conforme Norma P-SI-001, e que serão submetidos à autoridade competente para medidas cabíveis citadas na mesma.
V - Senha de acesso:
a) As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais do IPSM são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;
b) O IPSM adota os seguintes padrões para geração de senhas de acesso a seus ativos/serviços de informação ou recursos computacionais:
c) A equipe da ATI será responsável por fornecer senhas de acesso inicial ao usuário, que deverá proceder com a troca imediata da mesma;
d) As senhas terão prazo de validade a ser definido pela ATI. Passado este prazo, os sistemas solicitarão automaticamente a troca da senha;
e) As senhas associadas às contas com privilégio não-administrativo serão compostas usando uma quantidade mínima de 08 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;
f) As senhas associadas às contas que possuem privilégio administrativo serão compostas usando uma quantidade mínima de 08(oito) dígitos, combinando letras maiúsculas e minúsculas, números;
g) Após 05 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário será bloqueada, assim permanecendo assim por, no mínimo, 30 (trinta) minutos;
h) Quando efetuada uma troca da senha, o usuário não poderá realizar nova alteração dentro de um prazo mínimo de 7 (sete) dias. Caso seja necessário realizar alteração dentro deste período, o usuário deverá solicitar o apoio da ATI;
i) Quando criada uma nova senha, usuários devem estar atentos as seguintes recomendações:
1 - Não utilizar nenhuma parte de sua credencial na composição da senha;
2 - Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;
3 - Não utilizar repetição ou sequencia de caracteres, números ou letras;
4 - Qualquer parte ou variação do nome – IPSM;
5 - Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.
VI - Autorização de acesso (privilégios de acesso):
a) A autorização e o nível permitido de acesso aos ativos/serviços de informação do IPSM é feita com base em perfis que definem o nível de privilégio dos usuários;
b) O acesso à ativos/serviços de informação é fornecido a critério do IPSM, que define permissões baseadas nas necessidades laborais dos usuários;
c) Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador. Solicitações deverão ser encaminhadas a ATI;
d) Para criação de contas de acessos a sistemas ou a acesso à rede do IPSM, a Chefia imediata deve solicitar a ATI, por intermédio de abertura de chamado no Site do IPSM, contendo os seguintes dados do Colaborador:
1- Nome completo;
2- Diretoria, Assessoria, Gerência ou Departamento que o Colaborador ficará alocado;
3- Telefone/Ramal;
4- Matricula ou Masp;
VII - Os usuários devem, ainda, observar as seguintes diretrizes:
a) A seu critério exclusivo, o IPSM poderá ativar uma cota para armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto (nuvem). Caso o usuário necessite de mais espaço, deverá realizar uma solicitação à ATI através dos canais formais e institucionais estabelecidos;
b) É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse do IPSM tanto na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem);
c) Os arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) do IPSM pessoais podem ser excluídos, após aviso prévio ao usuário, pois todos são monitorados e auditados pela ATI. Caso sejam detectados arquivos pessoais ou em desacordo com a Política de Segurança do IPSM, será solicitado pela ATI a remoção ou exclusão pelo dono do arquivo.
VIII - É responsabilidade da ATI – Assessoria de Tecnologia da Informação:
a) Autorizar a concessão e revogação de acesso a ativos/sistemas de informação sob sua responsabilidade;
b) Autorizar a concessão e o controle de acesso administrativo a ativos/sistemas de informação sob sua responsabilidade;
c) Realizar a revisão periódica de autorizações de acesso e credenciais de acesso a ativos/sistemas de informação sob sua responsabilidade;
d) Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários de colaboradores, terceiros/prestadores de serviços;
e) Conceder, quando autorizado, o acesso aos usuários de colaboradores, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;
f) Revogar, quando solicitado, o acesso dos usuários de colaboradores, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;
g) Apoiar a revisão periódica da validade de credenciais de acesso aos ativos/sistemas de informação dos usuários e colaboradores, terceiros/prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.
IX - É responsabilidade do Departamento de Recursos Humanos - DRH:
a) Realizar o registro do desligamento dos colaboradores do IPSM no sistema destinado a essa finalidade para que a ATI receba a notificação e proceda com a exclusão devida dos acessos;
b) Apoiar a gestão de identidades dando a devida manutenção no sistema destinado a essa finalidade enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posição no IPSM;
c) Apoiar a revisão periódica da validade de credenciais de acesso aos ativos/sistemas de informação fornecendo informações sobre os colaboradores.
X- É responsabilidade dos Gerentes e Chefes de Departamento:
a) Solicitar a ATI através dos canais formais e institucionais estabelecidos a concessão e a revogação de acessos de novos colaboradores, servidores ou empregados, colaboradores e servidores que necessitem de novos acessos conforme mudanças em suas atividades laborais, ou por desligamento do setor ou do IPSM;
b) Solicitar ATI através dos canais formais e institucionais estabelecidos a concessão e a revogação de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso aos ativos/sistemas de informação ou por desligamento do setor ou do IPSM;
c) Informar a equipe da ATI quando ao encerramento do contrato com terceiros/prestadores de serviços contratados e colaboradores em geral que tenham a ativos/sistemas de informação.
Art. 5º - DO ACESSO A INTERNET E COMPORTAMENTO EM MÍDIAS SOCIAIS - N-SI-004
I - A Norma de segurança da informação N-SI-004 complementa Política de Segurança da Informação, definindo as diretrizes para utilização segura do acesso à internet fornecido pelo IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS BRASIL e do comportamento de colaboradores em mídias e redes sociais.
II - A norma tem propósito de estabelecer diretrizes para utilização segura do acesso à internet fornecido pelo IPSM e do comportamento de colaboradores em mídias e redes sociais.
III - Esta norma obedece ao escopo definido na Política de Segurança da Informação.
IV - Acesso à internet:
a) O IPSM fornece acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais . O usuário deverá utilizar a Internet em conformidade com a lei, a ordem pública e o Código de Conduta Ética do Agente Público e da Alta Administração Estadual;
b) O acesso à internet pode ser fornecido tanto através da rede corporativa do IPSM, quanto através da disponibilização de serviços de internet móvel, prestados por terceiros, contratados pelo IPSM;
c) O Acesso à internet por meio da rede wifi será disponibilizado aos colaboradores, conforme, solicitação dos Chefes de Departamentos, Gerentes, Assessores e Diretores;
d) Toda informação que é acessada, transmitida, recebida ou produzida através do acesso à internet fornecido pelo IPSM está sujeita ao monitoramento;
e) Caso o usuário esteja utilizando de forma excessiva a banda da internet, o mesmo será avisado e notificado pela ATI, para esclarecimento;
f) Na identificação da conduta irregular por parte do usuário, será submetido à Autoridade Competente para medidas cabíveis citadas nesta Política de Segurança da Informação;
g) Durante o monitoramento realizado pela ATI do IPSM, se resguarda o direito de efetuar o bloqueio da conta do Usuário, para fins de segurança;
h) Durante o acesso à Internet fornecido pelo IPSM não será permitido o download, o upload, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento e/ou a cópia de qualquer conteúdo relacionado expressa ou subjetivamente, direta ou indiretamente, com:
1 - Qualquer espécie de exploração sexual;
2 - Qualquer forma de conteúdo adulto, erotismo, pornografia;
3 - Qualquer tipo de Pornografia infantil;
4 - Qualquer forma de ameaça, chantagem e assédio moral ou sexual;
5 - Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;
6 - Preconceito baseado em cor, sexo, orientação sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;
7 - Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam essas lícitas ou não;

8 - A prática e/ou a incitação de crimes ou contravenções penais;
9 - A prática de propaganda política nacional ou internacional;
10 - A prática de quaisquer atividades comerciais desleais;
11 - Qualquer conteúdo protegido por direitos autorais;
12 - O desrespeito a imagem ou aos direitos de propriedade intelectual do IPSM;
13 - A disseminação de códigos maliciosos e ameaças virtuais;
14 - Tentativa de expor a infraestrutura computacional do IPSM a ameaças virtuais;
15 - Divulgação não autorizada de qualquer informação do IPSM, classificada como confidencial ou de uso interno;
16 - Uso de sites ou serviços que busquem contornar controles de acesso à internet.
V - Publicação de Conteúdo no Site do IPSM:
a) A publicação de conteúdo no site IPSM e de responsabilidade específica da ATI, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da organização;
VI - É responsabilidade da ATI - Assessoria de tecnologia da informação:
a) Controlar e monitorar qualquer tipo de acesso à internet fornecido pelo IPSM;
b) Reportar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso a internet à Diretoria.
Art. 6º - DO USO DE SERVIÇOS DE EMAIL E COMUNICADORES INSTANTÂNEOS - N-SI-005
I - A Norma de segurança da informação N-SI-005 complementa Política de Segurança da Informação, definindo as diretrizes para utilização dos serviços de e-mail e comunicadores instantâneos fornecidos pelo IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS.
II - O propósito é Estabelecer diretrizes para utilização segura dos serviços de e-mail e comunicadores instantâneos fornecidos pelo IPSM.
III - Esta norma obedece ao escopo definido na Política de Segurança da Informação.
IV - Serviço de E-mail:
a) O IPSM fornece o serviço de e-mail para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais;
b) Não é permitido o uso de qualquer serviço de e-mail, que não seja o oficialmente fornecido pelo IPSM;
c) Quando o usuário fizer uso do serviço de e-mail do IPSM, não é permitido:
1 - Utilizar do serviço de e-mail em caráter pessoal ou para fins que não sejam de interesse do IPSM;
2 - Utilizar de termos ou palavras de baixo calão na redação de mensagens;
3 - Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para endereços eletrônicos que não fazem parte do domínio corporativo do IPSM, excetuando-se quando expressamente autorizados;
4 - Inscrever o endereço de e-mail do IPSM em listas de distribuição e grupos de discussão que não estejam relacionadas com atividades laborais ou do interesse da organização;
5 - Fazer uso de qualquer técnica de falsificação ou simulação de falsa identidade e manipulação de cabeçalhos de e-mail. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas onde o Comitê Gestor de Segurança da Informação, notificará à autoridade competente que analisará a aplicação das sanções e punições previstas na Política de Segurança da Informação, e, nos casos de servidores podendo gerar um processo interno para avaliação;
6 - Tentar a interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;
7 - Utilizar o serviço de e-mail para o envio de mensagens indesejadas (spam) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de e-mail;
8 - Usar o serviço de e-mail para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;
9 - Usar o envio de material e mensagens de natureza ou com conteúdo racista, profana, obscena, intimidadora, difamatória, ilegal, ofensiva, abusiva, não ética, comercial, estritamente pessoal, de entretenimento, spam, com caráter eminentemente associativo, sindical, religioso, político e partidário, assim como qualquer outro que possa infringir a legislação vigente;
10 - Usar o serviço de e-mail para disseminar ou transmitir mensagens com conteúdo de cunho de propriedade autoral;
d) O serviço de e-mail do IPSM é continuamente monitorado para segurança, para fins de auditoria e verificação de sua devida utilização;
e) Na ocorrência de evidências de uso irregular do serviço de correio eletrônico, o IPSM efetuará registro do incidente de segurança da informação e notificará a Autoridade Competente, que decidirá sobre o processo de abertura de sindicância administrativa, com auditoria nas contas dos usuários sob suspeita, a fim de averiguar e garantir a segurança de toda a infraestrutura de tecnologia da informação e comunicação, bem como resguardar os objetivos, com base nas legislações vigentes;
f) O monitoramento do serviço de e-mail do IPSM tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como cumprir à legislação em vigor;
h) Na identificação da conduta irregular por parte do usuário, será submetido à Autoridade Competente para medidas cabíveis citadas nesta Política de Segurança da Informação;
i) Durante o monitoramento realizado pela ATI do IPSM, se resguarda o direito de efetuar o bloqueio da conta do Usuário, para fins de segurança;
j) O IPSM adota um padrão para criação dos endereços de E-mail sendo composto pelo primeiro nome do empregado, seguido por pontuação e seu último sobrenome, conforme exemplo a seguir:
1 - Nome completo do empregado: Marco de Araújo Soares;
2 - Email: marco.soares@ipsm.gov.br;
k) Casos de endereços de e-mail coincidentes ou que possam ocasionar cacofonias e situações vexatórias poderão ser alterados para seguir um modelo fora do padrão adotado pelo IPSM, devendo primeiramente ser revisados pela equipe da ATI;
l) Os usuários do serviço de e-mail do IPSM devem adotar a assinatura padrão, formatada de acordo com o seguinte:
1 - Modelo:
• Nome Completo
• Nome do departamento | sigla do departamento
• Nome da diretoria | sigla da diretoria
• Nome do Instituto completo
• Endereço do Instituto completo
• Telefone de contato do Instituto | site do Instituto
2 - Exemplo:
• Marco de Araújo Soares
• Assessoria de Tecnologia da Informação | ATI
• Diretoria Geral | DG
• IPSM -Instituto de Previdência dos Servidores Militares
• Rua Paraíba, 576 | 30130-140 | Belo Horizonte - MG | Brasil
• Tel.: +55 31 3269-20XX | www.ipsm.gov.br
3 - Ao final do e-mail, após a assinatura, deverá ser exibido o seguinte aviso de confidencialidade:
• O endereço (@ipsm.gov.br) é exclusivamente para as atividades profissionais de recepção e distribuição de informações. Lembre-se que o e-mail fornecido pelo IPSM é uma ferramenta de trabalho e pertencente à instituição.
• Esta mensagem é destinada exclusivamente a seu destinatário e pode conter informações privadas, privilegiadas e confidenciais. Se você a recebeu por engano, por favor, notifique imediatamente o remetente e elimine-a de seu computador. Qualquer disseminação, distribuição ou cópia desta comunicação é estritamente proibida.
• Antes de Imprimir, pense sobre sua responsabilidade social. Menos papel, mais árvores!
j) Para criação de contas de e-mails, a Chefia imediata deve solicitar a ATI, por intermédio de abertura chamado no Site, contendo os seguintes dados do Colaborador:
1 - Nome completo;
2 - Diretoria, Assessoria, Gerência ou Departamento que o Colaborador ficará alocado;
3 - Telefone/Ramal;
4 - Matricula ou Masp;
V - Serviços de Comunicadores instantâneos:
a) O IPSM disponibiliza o serviço de comunicadores instantâneos para seus usuários autorizados, exclusivamente para o desempenho de suas atividades profissionais;
b) Não é permitido o uso de qualquer serviço de comunicadores instantâneos, que não sejam oficialmente disponibilizados ou liberados pelo IPSM;
c) Quando o usuário fizer uso do serviço de comunicadores instantâneos do IPSM, não é permitido:
1 - Utilizar do serviço de comunicadores instantâneos em caráter pessoal ou para fins que não sejam de interesse do IPSM;
2 - Utilizar de termos ou palavras de baixo calão na redação de mensagens;
3 - Enviar informação classificada como de USO INTERNO ou CONFIDENCIAL para pessoas ou entidades que não fazem parte do domínio corporativo do IPSM, excetuando-se quando expressamente autorizados;
4 - Fazer uso de qualquer técnica forja ou simulação de falsa identidade. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme decisão do Comitê Gestor de Segurança da Informação;
5 - A interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;
6 - A utilização do serviço de comunicadores instantâneos para o envio de mensagens indesejadas (SPAM) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de comunicadores instantâneos;
7 - Usar o serviço de comunicadores instantâneos para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;
d) O usuário é o responsável exclusivo pelo uso inadequado de sua conta no serviço de comunicação instantânea, não sendo permitido o envio de mensagens cujo conteúdo incite uso de drogas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;
e) O serviço de comunicadores instantâneos é continuamente monitorado pelo IPSM, para fins de auditoria e verificação de sua devida utilização;
f) Na ocorrência de evidências de uso irregular deste serviço, o IPSM efetuará registro do incidente de segurança da informação e notificará a Autoridade Competente, que decidirá sobre o processo de abertura de sindicância administrativa, com auditoria nas contas dos usuários sob suspeita, a fim de averiguar e garantir a segurança de toda a infraestrutura de tecnologia da informação e comunicação, bem como resguardar os objetivos, com base nas legislações vigentes;
g) O monitoramento do serviço de comunicadores instantâneos do IPSM tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como cumprir à legislação em vigor;
h) Na identificação da conduta irregular por parte do usuário, será submetido à Autoridade Competente para medidas cabíveis citadas nesta Política de Segurança da Informação
i) Durante o monitoramento realizado pela ATI do IPSM, se resguarda o direito de efetuar o bloqueio da conta do Usuário, para fins de segurança.
VI - É responsabilidade da ATI - Assessoria de tecnologia da informação:
a) Controlar e monitorar os serviços de e-mail e comunicadores instantâneos fornecidos pelo IPSM;
b) Reportar ao CGSI eventuais tentativas de violação dos termos desta norma ou incidentes de segurança relacionados ao uso dos serviços de e-mail e comunicadores instantâneos.
VII - É responsabilidade do CGSI:
a) Avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria.
Art. 7º - DA PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS - N-SI-006
I - A Norma de segurança da informação N-SI-006 complementa Política de Segurança da Informação, definindo as diretrizes para proteção dos ativos/serviços de informação do IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS contra ameaças e códigos maliciosos de qualquer natureza.
II - O propósito Estabelecer diretrizes para a proteção dos ativos/serviços de informação do IPSM contra ameaças e códigos maliciosos de qualquer natureza.
III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, constante no Art. 2º desta Portaria.
IV - Ferramenta de proteção contra códigos maliciosos:
a) O IPSM disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos tais como vírus, cavalos de Tróia, vermes, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares;
b) Apenas a ferramenta disponibilizada pelo IPSM deve ser utilizada na proteção contra códigos maliciosos;
c) A ferramenta de proteção contra códigos maliciosos do IPSM adota as seguintes regras de uso:
1 - Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e varredura diária em estações de usuários e servidores corporativos;
2 - As varreduras semanais analisam todos os arquivos em cada uma das unidades de armazenamento locais das estações de usuários.
d)As varre duras diárias em servidores corporativos podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;
e) As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações;
f) Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários;
g) Caso uma estação de usuário esteja infectada ou com suspeita de infecção de código malicioso, a mesma deverá ser imediatamente isolada da rede corporativa do IPSM e de qualquer comunicação com a internet;
h) Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento do mesmo da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor;
V - Prevenção dos usuários contra códigos maliciosos:
a) Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários do IPSM devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos;
b) Os usuários do IPSM devem seguir as seguintes regras para proteção contra códigos maliciosos:
1 - Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;
2 - Reportar imediatamente a ATI qualquer infecção ou suspeita de infecção por código malicioso;
3 - Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;
4 - Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecidos pelo IPSM antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;
5 - Não habilitar MACROS para arquivos recebidos de fontes suspeitas, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio da equipe de segurança da informação para validar se o arquivo representa ou não uma ameaça.
VI - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:
a) Tratar casos de infecção ou suspeita de infecção por códigos maliciosos, reportando os mesmos a ATI, caso necessário;
b) Garantir que novas modalidades de códigos maliciosos são adequadamente investigados, tratados e protegidos pela ferramenta corporativa adotada pela IPSM;
c) Garantir a existência de iniciativas para divulgação sobre informações de ameaças, códigos maliciosos e medidas de proteção para os usuários da IPSM.
Art. 8º - DO USO DE EQUIPAMENTOS COMPUTACIONAIS PESSOAIS - N-SI-007
I - A Norma de segurança da informação N-SI-007 complementa Política de Segurança da Informação, definindo as diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo do IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS ou para o manuseio de informações do IPSM.
II - O propósito é estabelecer diretrizes para utilização segura de dispositivos computacionais pessoais no ambiente corporativo do IPSM ou para o manuseio de informações do IPSM.
III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, constante no Art. 2º desta Portaria.
IV - Uso de equipamentos computacionais pessoais no ambiente corporativo:
a) Entende-se por equipamento pessoal todo o dispositivo que não foi fornecido pelo IPSM para o desenvolvimento das atividades profissionais;
b) O IPSM fornece todos os recursos computacionais necessários para que seus colaboradores executem suas atividades laborais;
c) Ao seu critério exclusivo, o IPSM poderá permitir o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade;
d) A permissão para o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações de sua propriedade é uma prerrogativa da diretoria do IPSM, devendo o usuário estar formalmente autorizado e concordar integralmente com os termos desta norma, antes de fazer uso de dispositivos pessoais no ambiente corporativo ou para manusear informações de propriedade do IPSM;
e) O uso não autorizado de qualquer dispositivo de computação pessoal no ambiente corporativo será considerado uma violação da Política de Segurança da Informação e tratado como um incidente de segurança da informação, estando o responsável sujeito as sanções previstas nesta Política;
f) O IPSM não será responsável por guardar, fornecer suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos pessoais;
g) O uso de dispositivos de computação pessoal para atividades de trabalho ou armazenamento de arquivos do IPSM não modifica a propriedade da organização sobre as informações criadas, armazenadas, enviadas, recebidas, modificadas ou excluídas. Permanecendo qualquer direito de propriedade intelectual com o IPSM;
h) Quando autorizados a praticar o uso de dispositivos de computação pessoais para execução de trabalho de atividades ou manuseio de informações do IPSM, usuários serão inteiramente responsáveis por garantir a segurança de seus dispositivos, devendo garantir que:
1 - O sistema operacional dos dispositivos de computação pessoal estará sempre atualizado e com todas as correções/melhorias de segurança aplicadas;
2 - Dispositivos de computação pessoal possuem ferramenta para prevenção de códigos maliciosos e garantem que as assinaturas de códigos maliciosos são ser atualizadas em tempo real e executam varreduras diariamente;
3 - Dispositivos de computação pessoal utilizam apenas softwares licenciados, preservando o direito autoral.
i) É permitida a utilização de dispositivo pessoal e conexão à rede corporativa alternativa do IPSM, desde que haja uma solicitação da Chefia Imediata e a autorização da área responsável pela ATI;
j) O IPSM definirá os recursos ou dados corporativos disponíveis nos dispositivos particulares;
k) O IPSM não se responsabiliza pelo uso de softwares sem licenças nos dispositivos pessoais conectados à rede corporativa;
l) É de inteira responsabilidade do usuário a configuração do dispositivo pessoal conforme as regras de segurança definidas pelo IPSM.
m) O IPSM poderá, sem aviso prévio, suspender a conexão do dispositivo pessoal com a rede corporativa em caso de suspeita de comprometimento de informações ou incidentes de segurança. Emcaso de comprovação da suspeita, o acesso será revogado e as devidas providências administrativas para apuração de responsabilidade deverão ser realizadas;
n) Por se tratar de dispositivo pessoal, é de inteira e exclusiva responsabilidade do proprietário quanto a segurança dos dados nele armazenados. Deve-se utilizar mecanismos de criptografia e backup dos dados existentes, bem como o uso de softwares de antivírus e firewall;
o) Por se tratar de dispositivo pessoal, e de inteira responsabilidade do Usuário a manutenção preventiva e corretiva do equipamento, sendo vedado a solicitação de manutenção aos colaboradores da ATI.
V - É responsabilidade da ATI - Assessoria de tecnologia da informação:
a) Controlar e monitorar e autorizar o acesso a dispositivos pessoais na rede do IPSM;
b) Reportar ao CGSI eventuais tentativas de violação dos termos desta norma ou incidentes de segurança relacionados ao destes dispositivos pessoais.
VI - É responsabilidade do CGSI:
a) Avaliar, aprovar ou negar solicitações para uso de dispositivos pessoais no ambiente corporativo, bem como avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria.
Art. 9º - DO ACESSO REMOTO - N-SI-008
I - A Norma de segurança da informação N-SI-008 complementa Política de Segurança da Informação, definindo as diretrizes para o acesso remoto aos ativos/serviços de informação e recursos computacionais do IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS.
II - Estabelecer diretrizes para o acesso remoto aos ativos/serviços de informação e recursos computacionais do IPSM, garantindo níveis adequados de proteção aos mesmos.
III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, previsto ao Art. 2º desta norma.
IV - Concessão e uso do acesso remoto para Colaboradores do IPSM:
a) O acesso remoto a ativos/serviços de informação e recursos computacionais do IPSM é restrito aos usuários que necessitem deste recurso para execução das atividades profissionais;
b) O Acesso remoto será disponibilizado para os colaborares, no exercício de suas atividades relacionadas ao IPSM. O IPSM reserva para si o direito de monitorar a utilização do acesso remoto disponibilizado. A instalação e configuração ficará a cargo da ATI;
c) A ATI não se responsabiliza pelo acesso remoto, por parte do Colaborador, fora do expediente normal de trabalho;
d) O usuário será o único responsável por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por terceiros de posse de suas credencias de acesso remoto;
e) O acesso remoto aos ativos/serviços de informação e recursos computacionais do IPSM será concedido com os privilégios mínimos necessários para execução de suas atividades laborais;
f) Equipamentos computacionais utilizados para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes da IPSM e firewall local ativo;
V - O usuário, no uso do Acesso Remoto, se responsabiliza em utilizar somente seu Computador Pessoal, a fim de evitar acessos não autorizados à rede do IPSM, bem como garantir a proteção contra códigos maliciosos;
VI - Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais que possam o acesso remoto ao ambiente da IPSM habilitado, o usuário responsável deverá informar imediatamente o ocorrido à ATI.
VII - Para criação e contas de acesso remoto, a Chefia imediata deve solicitar à ATI, por intermédio de abertura de chamado no site do IPSM, contendo os seguintes dados do Colaborador:
1 - Nome completo;
2 - Diretoria, Assessoria, Gerência ou Departamento que o Colaborador ficará alocado;
3 - Telefone/Ramal;
4 - Matricula ou Masp;
VIII - Concessão e uso do acesso remoto terceiros:
a) O acesso remoto aos ativos/serviços de informação e recursos computacionais do IPSM poderá ser concedido pela ATI a terceiros ou prestadores de serviço, caso seja necessário para suas atividades laborais;
b) Para concessão e uso do acesso remoto para terceiros, devem ser observadas as seguintes regras:
1 - O acesso remoto de terceiros e prestadores de serviço aos ativos/serviços de informação ou recursos computacionais do IPSM somente poderá ser concedido após a efetivação e assinatura da Política de Segurança da Informação e a assinatura do acordo de confidencialidade entre as partes;
2 - A concessão do acesso deverá ser limitada automaticamente ao tempo necessário estimado a atividade do terceiro ou prestador de serviço;
3 - O usuário terceiro, bem como a empresa onde o mesmo trabalha, serão os únicos responsáveis por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por outras partes de posse de suas credencias de acesso remoto;
c) O acesso remoto de terceiros aos ativos/serviços de informação e recursos computacionais do IPSM será concedido com os privilégios mínimos necessários para execução de suas atividades laborais;
d) Equipamentos computacionais utilizados por terceiros para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes da IPSM e firewall local ativo;
e) O usuário terceiro, no uso do Acesso Remoto, se responsabiliza em utilizar somente seu Computador Corporativo, a fim de evitar acessos não autorizados à rede do IPSM, bem como garantir a proteção contra códigos maliciosos;
f) Em casos de acesso não autorizado, extravio, furto ou roubo de dispositivos computacionais de terceiros que possam o acesso remoto ao ambiente da IPSM habilitado, o usuário responsável deverá informar imediatamente o ocorrido a ATI;
g) Toda informação que é acessada, transmitida, recebida ou produzida através do acesso remoto aos ativos/serviços de informação ou recursos computacionais do IPSM é continuamente monitorado pelo IPSM;
h) Na ocorrência de evidências de uso irregular deste serviço, o IPSM efetuará registro do incidente de segurança da informação e notificará a Autoridade Competente, que decidirá sobre o processo de abertura de sindicância administrativa, com auditoria nas contas do Usuário sob suspeita, a fim de averiguar e garantir a segurança de toda a infraestrutura de tecnologia da informação e comunicação, bem como resguardar os objetivos com base nas legislações vigentes;
i) Durante o monitoramento do acesso remoto aos seus ativos/serviços de informação ou recursos computacionais, o IPSM se resguarda o direito de notificar ou avisar o usuário;
j) Na identificação da conduta irregular por parte do usuário, será submetido à Autoridade Competente para medidas cabíveis citadas nesta Política de Segurança da Informação;
k) Durante o monitoramento realizado pela ATI do IPSM, se resguarda o direito de efetuar o bloqueio da conta do Usuário, para fins de segurança;
IX - Para criação e contas de acesso remoto a pessoal externo ao IPSM, a Chefia imediata deve solicitar a ATI, por intermédio de abertura de chamado no Site do IPSM, contendo os seguintes dados do Colaborador:
1 - Nome completo;
2 - Justificativa pelo acesso remoto e o período a ser concedido;
3 - Diretoria, Assessoria, Gerência ou Departamento que o Colaborador que estará atuando;
4 - Telefone pessoal ou Corporativo;
X - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:
a) Avaliar, aprovar ou negar solicitações para uso de acesso remoto a ativos/serviços de informação ou recursos computacionais do IPSM;
b) Controlar e monitorar qualquer tipo de acesso remoto fornecido pelo IPSM;
c) Tratar eventuais tentativas de acesso não autorizados ou incidentes de segurança relacionados ao acesso remoto e, quando pertinente, reportar os mesmos ao CGSI.
XI - É responsabilidade do CGSI:
a) Avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria.
Art. 10 º - DO MONITORAMENTO DE ATIVOS E SERVIÇOS DA INFORMAÇÃO - N-SI-009
I - A Norma de segurança da informação N-SI-009 complementa Política de Segurança da Informação, definindo as diretrizes para o monitoramento de ativos/serviços de informação e recursos computacionais do IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS.
II - O propósito é estabelecer diretrizes para o monitoramento de ativos/serviços de informação e recursos computacionais do IPSM, garantindo o respeito dos usuários às regras estabelecidas na Política de Segurança da Informação, bem como produzir prova de eventual violação das condições constantes da mesma, e na legislação vigente.
III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, contida no Art. 2º desta Portaria..
IV - Monitoramento de ativos/serviços da informação e recursos computacionais:
a) Qualquer ativo/serviço de informação ou recurso computacional do IPSM, bem como qualquer outro recurso computacional com acesso aos mesmos, poderá ser monitorado a qualquer momento;
b) Todos os ativos/serviços de informação, recursos computacionais do IPSM, bem como toda informação trafegada ou armazenada nos mesmos, incluindo conta de e-mail corporativa e a navegação em sites e serviços da Internet são monitorados pelo IPSM;
c) O IPSM se resguarda o direito de notificar ou avisar o usuário sobre as ilegalidades a serem ocorridas, onde haverá bloqueio da conta do Usuário, que após procedimento administrativo, o IPSM poderá verificar o conteúdo da Conta;
d) Na utilização dos ativos/serviços de informação ou recursos computacionais do IPSM, incluindo a utilização da conta de e-mail corporativa, comunicadores instantâneos e navegação em sites da Internet, através da infraestrutura tecnológica do IPSM, o monitoramento tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como cumprir à legislação em vigor;
e) Durante o monitoramento dos serviços, o IPSM se resguarda o direito de notificar ou avisar o usuário sobre as ilegalidades a serem ocorridas nos ativos/serviços de informação ou recursos computacionais do IPSM, onde haverá bloqueio da conta do Usuário;
f) O IPSM efetuará registro do incidente de segurança da informação e notificará a Autoridade Competente, que decidirá sobre o processo de abertura de sindicância administrativa, com auditoria nas contas do Usuário sob suspeita, a fim de averiguar e garantir a segurança de toda a infraestrutura de tecnologia da informação e comunicação, bem como resguardar os objetivos com base nas legislações vigentes;
g) Durante o monitoramento dos ativos/serviços de informação ou recursos computacionais, o IPSM se resguarda o direito de notificar ou avisar o usuário;
h) Na identificação da conduta irregular por parte do usuário, será submetido à Autoridade Competente para medidas cabíveis citadas nesta Política de Segurança da Informação;
i) Durante o monitoramento realizado pela ATI do IPSM, se resguarda o direito de efetuar o bloqueio da conta do Usuário, para fins de segurança.
V - Do aviso legal:
a) O IPSM faz uso de um aviso legal para garantir que usuários e demais pessoas e entidades que tentem obter acesso aos ativos/serviços de informação ou recursos computacionais da organização estejam cientes das regras de segurança adotadas pelo IPSM, bem como do monitoramento realizado nos termos desta norma;
b) O aviso legal deverá ser exibido antes de permitir o acesso aos ativos/serviços de informação ou recursos computacionais do IPSM, apresentando o seguinte formato:
• "Este é um ativo/serviço de informação ou recurso computacional do IPSM, o qual pode ser acessado e utilizado somente por usuários previamente autorizados. Em caso de acesso e uso não autorizado ou indevido deste sistema, o usuário estará sujeito sanções cabíveis nas legislações aplicáveis. Este ativo/serviço de informação ou recurso computacional é monitorado. O acesso a este ativo/serviço de informação ou recurso computacional ou o uso do mesmo por qualquer pessoa ou entidade, autorizada ou não, constitui seu consentimento irrestrito aos termos aqui expostos."
c) O acesso a qualquer ativo/serviço de informação ou recurso computacional do IPSM ou o uso dos mesmos por qualquer pessoa ou entidade, autorizada ou não, caracteriza consentimento irrestrito aos termos expostos no aviso legal;
d) A ausência do aviso legal em qualquer ativo/serviço de informação ou recurso computacional do IPSM não descaracteriza a necessidade de cumprimento das regras expostas nas políticas, normas e demais procedimentos de segurança da informação adotados pelo IPSM.
VI - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:
a) Realizar o monitoramento dos ativos/serviços de informação ou recursos computacionais do IPSM;
b) Tratar eventuais violações das diretrizes de segurança do IPSM identificadas através de ferramentas de monitoramento, e, quando pertinente, reportar as mesmas ao CGSI.
VII - É responsabilidade do CGSI:
a) Avaliar irregularidades reportadas pela ATI e, havendo necessidade, reportar à Diretoria.
Art. 11º - DA RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO - N-SI-010
I - A Norma de segurança da informação N-SI-010 complementa Política de Segurança da Informação, definindo as diretrizes para responder eventos ou incidentes de segurança estejam impactandoou possam vir a impactar ativos/serviços de informação ou recursos computacionais do IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS.
II - O propósito é estabelecer diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informaçãoque possam impactar ativos/serviços de informação ou recursos computacionais do IPSM.
III - Esta norma obedece ao escopo definido na Política de Segurança da Informação, constante no Art. 2º da Portaria.
IV - Incidentes de segurança da informação:
a) Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais do IPSM serão caracterizadas

como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados;
b) Incidentes de segurança devem ser priorizados com base na criticidade dos ativos/serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista;
c) Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados a ATI;
d) A ATI deverá determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas;
e) Na ocorrência de um incidente de segurança da informação, ativos/ serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente;
f) A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados;
g) Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.
V - Time de resposta a incidentes de segurança da informação:
a) O time de resposta a incidentes de segurança da informação do IPSM deverá ser composto por, no mínimo, representantes das seguintes áreas:
1 - Assessoria de Tecnologia da Informação;
2 - Comitê Gestor de Segurança Da Informação
3 - Procuradoria.
b) Conforme a natureza do incidente, colaboradores de qualquer setor do IPSM podem ser convocados a participar do time de resposta a incidentes de segurança da informação;

c) O time de segurança da informação será concebido nos casos reais

de violação de segurança, ficando a cargo do CGSI em conjunto com a Diretoria do IPSM a designação de seus integrantes.
VI - Disseminação de informação sobre incidentes de segurança da informação:
a) Nenhum tipo de informação sobre incidentes e ocorrências de

segurança da informação poderá ser divulgado para entidades ou pessoas

externas ao IPSM sem aprovação expressa e formal da diretoria.
VII - É responsabilidade da ATI - Assessoria de Tecnologia da Informação:
a) Atuar como responsável por ocorrências e eventos de segurança e garantir a existência de recursos, identificar, escalar, mitigar, conter, e erradicar incidentes de segurança, bem como ações efetivas para recuperar o estado anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente.
b) Comunicar prontamente o time de resposta a incidentes de segurança da informação do IPSM, caso houver, sobre eventos e incidentes de segurança.
c) Apoiar no tratamento de ocorrências e incidentes de segurança da informação, fornecendo orientação e direcionamento estratégico dentro da área de especialidade de cada um dos participantes do time de resposta aos incidentes de segurança da informação;
d) Aconselhar a diretoria do IPSM sobre quais informações sobre eventos e incidentes de segurança da informação podem ser divulgadas para públicos internos e externos.
VIII - É responsabilidade da Procuradoria:
a) No que couber, apoiar nas respostas administrativas e atuações judiciais necessárias conforme identificação da ocorrência.
IX - É responsabilidade do CGSI:
a) Apoiar na identificação dos possíveis vazamentos e no plano de respostas ao incidente;
b) Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público;
c) Elenca, em conjunto com a Diretoria do IPSM, nos termos do Inciso V deste Artigo, servidores para analisar as violações de segurança, ocorridas no IPSM, nos temos desta Política de Segurança da Informação, bem como auxiliar a Diretoria na elaboração da resposta ao incidente.
Art. 12º - Sanções serão avaliadas conforme previsto na Política de Segurança da Informação e normas complementares, e que serão submetidos à Autoridade Competente para medidas cabíveis citadas na mesma.
Art. 13º - Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.
Art. 14º - A Portaria é aprovada pela Diretoria do IPSM - INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MILITARES DO ESTADO DE MINAS GERAIS.
Art. 15º - Esta Portaria entra em vigor na data de sua publicação.

Belo Horizonte, 11 de agosto de 2023.
(a) Fabiano Villas Boas, Cel. PM QOR
Diretor-Geral do IPSM

16 1830249 - 1

partir de 28/7/23, em prorrogação.