DDoS, provocar congestionamento em redes, tentativas deliberadas de sobrecarregar ou invadir um servidor.
XVI .conectar equipamentos particulares à rede corporativa sem prévia autorização.
XVII .acessar as estações de trabalho sem autorização do responsável pela unidade.
XVIII .movimentar as estações de trabalho, periféricos e ou equipamentos de rede sem autorização do responsável pelo setor de TIC.
XIX .incluir senhas em processos automáticos, como por exemplo, em arquivos de dados, programas de computador, macros, scripts, ferramentas, teclas de função ou outros, exceto se autorizado pela área de Segurança da Informação e desde que, comprovadamente, não haja comprometimento à segurança da informação.
XX .armazenar informações corporativas do Estado em diretórios (pastas) públicos (as).
Art 47É vedada a conexão de dispositivos não autorizados na rede local, principalmente, equipamentos de rede sem fio como Access Points, modem ou qualquer outra solução que estabeleça conexão simultânea com a rede local e outras redes.
Parágrafo Único. Em casos justificados de uso destes equipamentos, o órgão ou entidade deverá prover segmento de rede independente, através de VLAN, para este fim, de forma a permitir o compartilhamento de sua infra-estrutura de TI sem o comprometimento do desempenho e da segurança da rede local.
CAPÍTULO XII – DAS RESPONSABILIDADES
Art 48Compete ao usuário:
I .obedecer e cumprir a Política de Segurança da Informação do Governo do Estado;
II .notificar à área responsável pela Segurança da Informação casos de suspeita ou violação das regras ou de falhas de segurança da informação;
III .sugerir medidas que possam elevar os níveis de segurança das instalações na sua área de atuação;
IV .utilizar e manter o crachá em local visível durante sua permanência nas instalações do órgão ou entidade;
V .avisar à chefia imediata ou ao superior a perda, furto ou o desaparecimento de crachás.
VI .informar à chefia imediata ou ao superior a presença de pessoas sem identificação nas instalações da órgão ou entidade.
VII .devolver o crachá ao término do contrato de trabalho nos casos de exoneração de cargo efetivo, aposentadoria ou desligamento do órgão ou entidade.
VIII .responder pelo uso de seu login de acesso aos sistemas e serviços do órgão ou entidade;
IX .zelar pelas informações, sistemas, serviços e recursos de tecnologia da informação sob sua responsabilidade;
X .não realizar alterações na configuração da estação de trabalho;
XI .utilizar adequadamente os recursos computacionais;
XII .conduzir adequadamente o uso da Internet, respeitando direitos autorais, regras de licenciamento de softwares, direitos de propriedade e privacidade;
XIII .alterar a senha no momento em que receber as informações da criação de sua conta;
XIV .manter sigilo de seu login e de sua senha de acesso aos sistemas e serviços do órgão ou entidade;
XV. trocar a senha sempre que houver indícios de comprometimento do sistema ou da própria senha;
XVI .guardar as mídias removíveis, contendo dados, em armários com chaves;
XVII .guardar os documentos em papel que contenham informações sigilosas de forma segura e em local fechado;
XVIII .não reproduzir documento sem a autorização do responsável pela informação;
XIX .imprimir documentos, caso sejam sigilosos, utilizando impressoras com proteção por meio de senhas ou permanecer próximo à impressora, no momento de sua emissão;
XX .não reutilizar documentos em papel que possuam conteúdos sigilosos, devendo estes serem descartados por meio de fragmentação;
XXI .eliminar os arquivos desnecessários armazenados nos servidores da rede do órgão ou entidade;
XXII .responder pelo uso de dispositivos particulares no ambiente do órgão ou entidade;
XXIII .solicitar à chefia imediata a utilização e a conexão do dispositivo móvel na rede corporativa justificando a sua necessidade;
XXIV .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;
XXV .ser responsável pelos dispositivos móveis, e pelos dados armazenados nos mesmos, disponibilizados para uso dentro e fora das instalações do órgão ou entidade;
XXVI .não deixar os dispositivos móveis desprotegidos em locais de alto risco, tais como locais públicos, eventos, hotéis, veículos, dentre outros;
XXVII .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 órgão ou entidade;
XXVIII .apresentar o dispositivo móvel para a área responsável pelo atendimento ao usuário, quando requisitado, ou ao cessar as atividades que motivaram sua solicitação;
XXIX .zelar pela guarda do dispositivo de armazenamento do certificado e pela senha de acesso ao dispositivo.
XXX .requisitar a revogação do certificado digital caso ele seja perdido, roubado ou extraviado, informando imediatamente o fato à área responsável.
Art 49Compete à área de TIC:
I .cumprir e fazer cumprir a Política de Segurança da Informação;
II .manter os sistemas computacionais e de comunicação em conformidade com a Política de Segurança da Informação;
III .disponibilizar os recursos necessários à implantação da Política de Segurança da Informação;
IV .manter os dados cadastrais dos usuários da rede corporativa, bem como do correio eletrônico, atualizados;
V .reportar incidentes de segurança da informação à área responsável pela Segurança da Informação;
VI .monitorar os logs dos sistemas;
VII .acompanhar a realização de manutenção, corretiva ou preventiva, dos servidores e subsistemas de armazenamento da rede corporativa do órgão ou entidade quando a manutenção for realizada por terceiros no ambiente do órgão ou entidade;
VIII .prestar suporte ao usuário quando solicitado;
IX .solicitar apoio e consultoria de segurança à área responsável pela Segurança da Informação quando se fizer necessário;
X .solicitar a assinatura do Termo de Responsabilidade do usuário pela estação de trabalho;
XI .instalar e configurar as estações de trabalho;
XII .manter um inventário atualizado das estações de trabalho e dos softwares;
XIII .desenvolver e manter um padrão de instalação e configuração de estações de trabalho aderente aos critérios estabelecidos nesta resolução;
XIV .configurar os programas de computador e equipamentos para garantir a utilização dos critérios relativos às senhas de acesso definidos pela área de Segurança da Informação;
XV .manter o antivírus, anti-spam e as correções de segurança dos servidores e estações de trabalho atualizados;
XVI .lacrar os microcomputadores;
XVII .documentar toda a infraestrutura de TIC do órgão ou entidade, tais como tipo de equipamento, patrimônio, localização física, data da aquisição, prazo de garantia, etc;
XVIII .controlar e descartar os Hard Disks (HDs) e mídias removíveis, quando necessário;
XIX .disponibilizar e administrar a infraestrutura necessária para armazenamento de dados;
XX .disponibilizar e administrar os recursos de acesso à Internet;
XXI .monitorar o uso da Internet;
XXII .registrar os acessos indevidos à Internet;
XXIII .orientar os usuários em relação à proteção adequada dos dispositivos móveis;
XXIV .configurar os dispositivos móveis disponibilizados para os usuários do órgão ou entidade;
XXV .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 órgão ou entidade;
XXVI .manter a documentação dos servidores, subsistemas de armazenamento, e programas de computador diretamente vinculados às soluções de backup e restore;
XXVII .realizar o backup e a remoção das informações armazenadas nos servidores e subsistemas de armazenamento da rede corporativa do órgão ou entidade, no caso de manutenção externa ao órgão ou entidade;
XXVIII .definir os recursos e ferramentas que serão utilizados em cada procedimento de backup e restore;
XXIX .documentar os procedimentos de backup e restore;
XXX .eliminar e substituir as mídias de backup e restore próximas de perderem sua funcionalidade segundo a vida útil informada pelo fornecedor;
XXXI .eliminar o conteúdo das mídias que serão descartadas;
XXXII .executar os procedimentos de backup e restore;
XXXIII .gerenciar e controlar os recursos computacionais e as mídias utilizadas pelos sistemas de backup e restore do órgão ou entidade;
XXXIV .manter mapa atualizado das mídias e seus conteúdos para todos os procedimentos de backup e restore do órgão ou entidade;
XXXV .planejar junto às áreas solicitantes os procedimentos de backup e restore;
XXXVI .realizar testes de validação e desempenho das cópias de segurança realizadas;
XXXVII .disponibilizar os recursos necessários para a execução das funções de auditoria;
XXXVIII .garantir a proteção adequada das trilhas de auditoria;
XXXIX .aprovar e registrar a utilização das ferramentas de monitoramento e acesso às estações de trabalho;
XL .analisar e despachar os expedientes relativos a solicitações de usuários encaminhadas pelos respectivos responsáveis por suas unidades;
XLI .administrar o acesso remoto à rede do órgão ou entidade;
XLII .definir os softwares autorizados que deverão ser instalados nas estações de trabalho;
XLIII .administrar as redes corporativas do órgão ou entidade;
XLIV .manter a documentação da topologia da rede atualizada e controlar o acesso ao seu conteúdo;
XLV .prover o ambiente físico necessário para instalação dos roteadores e switches;
XLVI .homologar e administrar os roteadores e switches do órgão ou entidade;
XLVII .manter a documentação (topologia, configurações, etc) dos roteadores e switches atualizada;
XLVIII .administrar as regras dos firewalls;
XLIX .instalar, configurar e manter os ambientes operacionais dos firewalls - sistema operacional nos servidores, bem como os produtos e as correções e atualizações de versão;
L.aplicar, anualmente, os controles disponibilizados pela ferramenta de gestão de riscos nos ativos em que estejam instalados os firewalls;
LI .manter atualizadas as documentações (configurações) relativas aos firewalls;
LII .disponibilizar a infraestrutura necessária para o funcionamento da solução de network IDS/IPS;
LIII .instalar e administrar o network IDS/IPS;
LIV .analisar periodicamente as logs dos Networks IDS em busca de incidentes de Segurança da Informação;
LV .avaliar, no mínimo trimestralmente, o desempenho do network IDS/IPS em relação à quantidade de ataques detectados, falsos positivos (alarme falso), carga da rede, entre outros;
LVI .manter a documentação do network IDS/IPS atualizada;
LVII .instalar, homologar, manter e configurar todos os equipamentos de conectividade que componham as soluções de backup e restore utilizadas no órgão ou entidade;
LVIII .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;
LIX .analisar e emitir parecer sobre as solicitações da área de segurança da informação;
LX .atualizar os controles da ferramenta de análise de risco de Segurança da Informação;
LXI .avaliar e aplicar, para as situações consideradas críticas, os controles existentes na ferramenta de análise de risco de Segurança da Informação;
LXII .elaborar e manter atualizado um procedimento de instalação e configuração da rede;
LXIII .administrar a cessão, a alteração, o bloqueio e o cancelamento de acessos à rede corporativa;
LXIV .revisar, pelo menos 1 (uma) vez por ano, os direitos de acesso dos usuários da rede corporativa e realizar as alterações necessárias;
LXV .revisar, pelo menos a cada 6 (seis) meses, os direitos de acesso com privilégios de administrador e realizar as alterações necessárias;
LXVI .definir, homologar, implementar e disponibilizar a infra-estrutura e os mecanismos de segurança para utilização da rede wireless;
LXVII .realizar semestralmente análise de risco na rede wireless;
LXVIII .disponibilizar relatório as conexões remotas realizadas.
LXIX .solicitar a autorização para movimentação patrimonial de ativos (hardware e software) à área de TIC;
Art 50Compete ao setor de auditoria:
I .realizar a auditoria nos sistemas do órgão ou entidade;
II .verificar a conformidade com o estabelecido nesta norma e recomendar as ações necessárias;
III .definir parâmetros de geração e retenção das trilhas de auditoria, juntamente com a área responsável pela Segurança da Informação, para fins de controle interno;
IV .gerar e manter atualizada a documentação das ferramentas e auditorias realizadas;
V .manter a área responsável pela Segurança da Informação informada sobre as ferramentas utilizadas;
VI .monitorar a utilização das userid de auditoria.
Art 51Compete à área de recursos humanos informar, mensalmente, à equipe de Segurança da Informação, a movimentação de pessoal no órgão ou entidade.
Art 52Compete à direção das unidades administrativas:
I .orientar os usuários sob sua coordenação sobre o cumprimento desta resolução e zelar pelo acesso aos sistemas e serviços do órgão ou entidade;
II .cumprir e fazer cumprir a Política de Segurança da Informação em relação aos seus subordinados;
III .monitorar as atividades de parceiros e contratados sob sua responsabilidade;
IV .colaborar com a área responsável pela Segurança da Informação na elaboração da Política de Segurança da Informação;
V .propor mudanças na Política de Segurança da Informação de acordo com as necessidades iminentes detectadas na sua área de atuação;
VI .reportar, de imediato, à área responsável pela Segurança da Informação, qualquer incidente de segurança detectado ou, até mesmo, qualquer suspeita ou ameaça de incidentes;
VII .avaliar a necessidade de utilização de dispositivo móvel particular e da conexão à rede corporativa do órgão ou entidade;
VIII .solicitar à área de TIC qualquer alteração nas condições autorizadas para a utilização de dispositivo móvel;
IX .solicitar as permissões de acesso para usuários sob sua subordinação à área executora que detenha o controle de acesso ao respectivo recurso computacional;
X .solicitar, com a devida justificativa, para área de TIC a instalação de softwares.
Art 53Compete à área responsável pela Segurança da Informação:
I .elaborar a Política de Segurança da Informação;
II .verificar o cumprimento desta Resolução e recomendar as ações preventivas e ou corretivas necessárias;
III .administrar, controlar e dar tratamento aos incidentes de segurança da informação;
IV .analisar e autorizar solicitação para conexão na rede corporativa de mídias ou dispositivo móvel particular nas dependências do órgão ou entidade;
V .autorizar, quando necessário, a criação de regras no firewall, considerando a análise de risco realizada;
VI .analisar e emitir parecer sobre as informações de incidentes de segurança ou inconformidades;
VII .aprovar controle de segurança;
VIII .avaliar e apresentar pareceres a respeito das exceções requeridas pelos responsáveis de unidades administrativas do órgão ou entidade;
IX .avaliar, periodicamente, a Segurança da Informação, por meio de análise de indicadores e recomendar ações corretivas e preventivas;
X .definir e padronizar os critérios das senhas de acesso à rede;
XI .elaborar campanhas e programas de treinamento e de conscientização em Segurança da Informação;
XII .elaborar relatórios gerenciais sobre o acesso à Internet;
XIII .elaborar, propor e coordenar projetos, ações e soluções de segurança da informação;
XIV .emitir relatório de alerta e incidente de segurança quando detectado acesso indevido à Internet;
XV .especificar padrão de configuração de segurança destinada a acesso remoto à rede corporativa;
XVI .garantir a implementação dos projetos e soluções de segurança da informação aprovados, atuando permanentemente em busca de parcerias com os diversos responsáveis pelos processos, visando à redução do índice de riscos do órgão ou entidade;
XVII .homologar junto à área de TIC os procedimentos de backup e restore;
XVIII .homologar padrões definidos pela área de redes;
XIX .homologar parâmetros de configuração dos IDS/IPS;
XX .homologar, autorizar e validar o uso de equipamentos e programas de computador nas estações de trabalho quando não existir licença de uso ou o software solicitado for desconhecido ou passível de risco de segurança;
XXI .priorizar as ações de segurança;
XXII .prover apoio técnico consultivo para as unidades administrativas do órgão ou entidade nas questões relativas à segurança da informação;
XXIII .recomendar a adoção de soluções emergenciais sobre segurança da informação;
XXIV .recomendar soluções, ferramentas ou recursos que viabilizem o monitoramento e o registro dos acessos à internet;
XXV .realizar análise de riscos em equipamentos, infraestrutura e pessoas;
XXVI .avaliar o nível de segurança alcançado, emitindo relatórios periódicos de Análise de Riscos à Diretoria e ao Comitê Gestor;
XXVII .definir e acompanhar a execução do Plano Estratégico para implantação da Política de Segurança da Informação;
XXVIII .definir e aprovar junto à alta gestão, os procedimentos e penalidades para se fazer cumprir a Política de Segurança;
XXIX .definir e solicitar os recursos necessários para implantação da Política de Segurança;
XXX .efetuar mudanças na Política de Segurança da Informação sempre que houver alteração no ambiente computacional ou atualizações tecnológicas, visando à manutenção e melhora do nível de segurança;
XXXI .realizar análise de risco para criação de regras no firewall e gerar laudo técnico;
XXXII .dar tratamento aos casos de exceção e aqueles não previstos nas normas relativas à segurança da informação.
XXXIII .aprovar, quando devido, as solicitações de acessos à rede corporativa com privilégios de administrador;
XXXIV .analisar os incidentes de segurança da informação e recomendar ações corretivas e preventivas;
XXXV .realizar, no mínimo anualmente, uma análise crítica dos direitos de acesso dos usuários sob sua coordenação e solicitar as alterações necessárias;
XXXVI .monitorar a utilização de mídias particulares para armazenamento de informações do órgão ou entidade;
XXXVII .tomar as providências cabíveis em caso de descumprimento da Política de Segurança da Informação por seus subordinados;
XXXVIII .analisar permanentemente os acessos remotos realizados por seus subordinados, através de relatório disponibilizado pela área de TIC;
XXXIX .receber, analisar e encaminhar a solicitação de permissão e revogação de acesso para o empregado ou prestador de serviço sob sua subordinação à área de TIC;
XL .informar, em caso de solicitações temporárias, o período em que a utilização da conexão permanecerá liberada, para visitantes e demais usuários;
XLI .avaliar as solicitações para o uso de dispositivo móvel de propriedade ou alugado pelo órgão ou entidade e requerer à área de TIC;
XLII .autorizar, quando necessário, a liberação de portas de diagnóstico remotas;
XLIII .autorizar acessos à rede;
XLIV .informar à Companhia de Tecnologia da Informação do Estado de Minas Gerais – Prodemge, pelo menos 2 gestores de segurança, que terão a função de tratar qualquer assunto relacionado a segurança da informação.
XLV .manter e publicar anualmente um programa de conscientização sobre a segurança da informação;
XLVI .informar anualmente à Superintendência Central de Governança Eletrônica - SCGE da Secretaria de Estado de Planejamento e Gestão - SEPLAG quais as ferramentas de segurança possuem, descrevendo pelo menos, a função, o fabricante, a versão utilizada e a indicação da existência de contrato de manutenção.
CAPÍTULO XIII – PENALIDADES
Art 54O usuário que não cumprir as normas estabelecidas nessa Resolução estará sujeito às penalidades previstas em Lei.
CAPÍTULO XIV – DISPOSIÇÕES FINAIS
Art 55Os Órgãos e Entidades do Poder Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional deverão adequar-se ao disposto nesta Resolução no período máximo de 1 (um) ano a partir de sua publicação.
Parágrafo Único. Compete à Secretaria de Estado de Planejamento e Gestão - Seplag, por meio da Superintendência Central de Governança Eletrônica, fornecer as orientações necessárias ao fiel cumprimento das regras dessa Resolução, além de verificar a conformidade das práticas com o estabelecido nesta Resolução e recomendar as correções necessárias.
Art 56Fica facultada, às Empresas Públicas e Sociedades de Economia Mista, a aplicação das regras contidas na presente Resolução, observada a conveniência e a oportunidade administrativas.
Art 57Caberá à Secretaria de Estado de Planejamento e Gestão, por meio da Subsecretaria de Gestão, esclarecer os casos omissos a esta Resolução.
Art 58Este Decreto entra em vigor na data de sua publicação, revogada a Resolução SEPLAG n° 73 de 21 de setembro de 2009.

Belo Horizonte, aos 26 de dezembro de 2018.
HELVÉCIO MIRANDA MAGALHÃES JUNIOR
Secretário de Estado de Planejamento e Gestão

26 1179282 - 1

DIRETORIA CENTRAL DE OPERAÇÃO
DA POLÍTICA DE CARREIRAS
Acumulação de Cargos, Empregos e Funções Públicos

A Diretora da Diretoria Central de Operação da Política de Carreiras, da Secretaria de Estado de Planejamento e Gestão, tendo em vista o disposto no art. 43, inciso I, alínea "d", do Decreto nº 47.337, de 12 de janeiro de 2018, faz saber aos interessados abaixo relacionados da decisão do estudo de seus processos de acumulação de cargos.
Decisão: acumulações lícitas, nos termos do artigo 37, inciso XVI, alíneas "a", "b" e "c"; artigo 37 § 10; art. 38, inciso III; artigos 42 e 142; artigo 95, parágrafo único, inciso I; artigo 128, § 5º, inciso II, alínea "d", todos da Constituição Federal de 1988, e artigo 17, §§ 1º e 2º dos Atos das Disposições Constitucionais Transitórias, da Constituição Federal de 1988, comprovada a compatibilidade das cargas horárias.
-FUNDAÇÃO HOSPITALAR DO ESTADO DE MINAS GERAIS:
SOFIA CORDEIRO PUBLIO -Masp 1234291-1, AGAS(FISIOTERAPEUTA RESPIRATORIA)/FISIOTERAPEUTA (FISIOTERAPEUTA - RIBEIRÃO DAS NEVES); DANIEL FREITAS DE ALMEIDA -Masp 1210597-9, AGAS(CIRURGIAO DENTISTA BUCOMAXILOFACIAL)/ODONTOLOGO CIRURGIAO(NOVA LIMA); SILVANA MATOS LOPES -Masp 1294600-0, AGAS(FONOAUDIOLOGO)/FONOAUDIÓLOGO (NOVA LIMA); FRANCISCO DE ASSIS RIBEIRO JUNIOR -Masp 1356202-0, MED(MEDICO OFTALMOLOGISTA)/PRIMEIRO TENENTE (MÉDICO - CBMMG); VICENTE DE PAULA GOMES -Masp 1041797-0, MED(MEDICO EM RADIOLOG.E DIAGNOST.POR IMAGEM)/MÉDICO (MÉDICO - VISCONDE DO RIO BRANCO); MARIELA RODRIGUES FERNANDES CAMPOS -Masp 1123866-4, MED(MEDICO CLINICO)/CONTRATO MEDICO - LEI 18185/2009. (MEDICO CLINICO).
-POLICIA CIVIL DO ESTADO DE MINAS GERAIS:
THOMAS MARTINS DE ALMEIDA -Masp 1163069-6, MEDICO LEGISTA/MÉDICO (MÉDICO PSIQUIATRA - TRT - 3ª REGIÃO).
-SECRETARIA DE ESTADO DE EDUCAÇÃO:
- SRE METROPOLITANA A:
TADEU GOMES SANTOS -Masp 1065714-6, PEB/PEB; ROBERVAL PINTO LIMA -Masp 0848375-2, PEB(EXERCENDO VICE-DIRECAO)/PROFESSOR(SABARÁ); ADRIANO MAURICIO CRUZ -Masp 0876487-0, PEB/PEB; MIRIA CHIRLEY DE OLIVEIRA -Masp 1408340-6, EEB/PROFESSOR(PIEDADE DOS GERAIS); MARCILENE MARIA DE ANDRADE -Masp 1219320-7, PEB/PEDAGOGO (PIEDADE DOS GERAIS); IANE APARECIDA DE RESENDE -Masp 1408303-4, PEB/PROFESSOR(PIEDADE DOS GERAIS); RUIVANY ZONFRILLY MOREIRA CAMPOS MARTINS -Masp 0536678-6, PEB/PROFESSOR(PIEDADE DOS GERAIS); MARCIA BERNARDINO -Masp 0977546-1, PEB/PROFESSOR(NOVA LIMA).
- SRE METROPOLITANA C:
MONICA MARCIA LOPES FRANCISCO DE OLIVEIRA -Masp 0983758-4, PEB/VICE-DIRETOR(PEDRO LEOPOLDO); MARIA DA GLORIA ALVES SANTOS -Masp 1286748-7, PEB/PROFESSOR(BELO HORIZONTE); MARIA APARECIDA DA SILVA ABREU -Masp 0974548-0, PEB/PROFESSOR(VESPASIANO); FLAVIANA ANTÔNIA DA CRUZ -Masp 1386899-7, PEB/PEDAGOGO (RIBEIRÃO DAS NEVES); AMANDA AZEVEDO DA SILVA ROMAO -Masp 1292023-7, PEB/PEB; LUIZ CARLOS DOS ANJOS MARSAL -Masp 1080087-8, PEB/FISCAL POSTURAS(LAGOA SANTA).
- SRE DE ALMENARA:
IVANETE PEREIRA DA SILVA -Masp 0557142-7, PROFESSOR(ÁGUAS VERMELHAS - CEDIDO)/PEB, exercendo por ambos DIRETOR V.
- SRE DE BARBACENA:
GILBERTO DEBORTOLI DELAROTA -Masp 1454511-5, PEB/PEB; ROSANA APARECIDA DE PAULA -Masp 1382575-7, PEB/PEB; MARIA BETHANIA LAGE -Masp 0887466-1, PEB(EXERCENDO SECRETARIO DE ESCOLA)/PROFESSOR II(SANTANA DO GARAMBÉU); CLAUDIA LUCIA CORREA NETO -Masp 0881317-2, PEB/PEB; SELMA ROSIMEIRE PAMPLONA -Masp 1410348-5, PEB/PROFESSOR(SENHORA DOS REMÉDIOS); WILMAR JOSE BELO DE ASSIS -Masp 0847082-5, PEB/PROFESSOR I(BARBACENA).
- SRE DE CAMPO BELO:
RAQUEL FLORIANO BERNARDES -Masp 1311250-3, EEB/PEB.
- SRE DE CARANGOLA:
PASCHOALINA MOREIRA PEDROSA -Masp 1181994-3, PEB/SUPERVISOR PEDAGÓGICO(SÃO FRANCISCO DO GLÓRIA).
- SRE DE CAXAMBU:
CELIA MARIA DA SILVA ROCHA -Masp 1177243-1, PEB/PROFESSOR(CRUZÍLIA).
- SRE DE CONSELHEIRO LAFAIETE:
ANA LUCIA FERREIRA -Masp 0937204-6, PEB/PROFESSOR DE EDUCAÇÃO BASICA(OURO BRANCO); JOSE AMANCIO FILHO -Masp 1431878-6, PEB/PROFESSOR II(CASA GRANDE); ELIETE VENTURA GONCALVES -Masp 0823404-9, PEB/VICE-DIRETOR ESCOLAR(CONGONHAS); MARLI VARELA DOS SANTOS ANDRADE -Masp 1152916-1, EEB/PROFESSOR(CONGONHAS).
- SRE DE CORONEL FABRICIANO:
ADAIL JOSE DE ANDRADE -Masp 1075904-1, PEB/PROFESSOR(BRAÚNAS); EVA VILMA GOMES -Masp 0979239-1, PEB/PEB; JANE ALMEIDA DE OLIVEIRA EUFRÁZIO -Masp 0551331-2, PEB/PEB(APOSTILA DIRETOR DE ESCOLA).
- SRE DE DIVINOPOLIS:
BRUNA APARECIDA SILVA PRIMO -Masp 1182123-8, PEB/PEB; REGINA ANTONIA DIAS OLIVEIRA -Masp 0374825-8, PEB(APOSENTADO)/PEB(EXERCENDO VICE-DIRECAO); DONIZETE DINIZ DA SILVA JUNIOR -Masp 1454402-7, PEB/PEB; SIMONE GLORIA COSTA RABELO -Masp 1406704-5, PEB/PEB; GILMAR SILVA RIBEIRO -Masp 1459435-2, PEB/PEB; FERNANDA CRISTINA DE OLIVEIRA -Masp 0891717-1, PEB/PROFESSOR(DIVINÓPOLIS).
- SRE DE GOVERNADOR VALADARES:
CASSIOS CAMPOS DE OLIVEIRA -Masp 1220773-4, PEB/PEB; GISLAINE APARECIDA DOS SANTOS -Masp 0864686-1, PEB/PEB(EXERCENDO SECRETARIO DE ESCOLA); SOLANGE BATISTA DE OLIVEIRA CORDEIRO -Masp 0638165-1, PEB(EM AFAST.PREL.)/PEB(EXERCENDO DIRETOR IV).
- SRE DE ITAJUBA:
ROBSON MAROTI JUNIOR -Masp 1428863-3, PEB/PEB; ANA BEATRIZ CORREA CAMPOS CARVALHO -Masp 0335927-0, PEB(APOSENTADO)/PEB.
- SRE DE ITUIUTABA:
REGIANE ANDRADE DE JESUS -Masp 1437977-0, PEB/PROFESSOR(SANTA VITÓRIA); LUCINDA MARIA SATURNO -Masp 0694531-5, PEB/PROFESSOR(CENTRALINA).
- SRE DE JANUARIA:
MARILIA MENDES GOMES -Masp 1293024-4, PEB/PEB; DULCINEA BISPO TORRES -Masp 0338595-2, PEB/PEB.
- SRE DE JUIZ DE FORA:
ADRIANA APARECIDA DE OLIVEIRA -Masp 1106988-7, PENF(TECNICO DE ENFERMAGEM)/PEB.
- SRE DE LEOPOLDINA:
JULIANA APARECIDA MAGALHAES DE SOUZA SOARES -Masp 1433541-8, PEB/PEB; ERCIO PINTO SOUZA -Masp 0075269-1, P5/P5.
- SRE DE MONTE CARMELO:
HELEN CARLA APARECIDA MENDES -Masp 1130558-8, PEB/PEB; MARTA MARIA DA ROCHA -Masp 1116093-4, PEB/PROFESSOR(MONTE CARMELO).
- SRE DE MONTES CLAROS:
EVA APARECIDA MIRANDA PEIXOTO -Masp 1058961-2, ATB/PROFESSOR(CRISTÁLIA)/VEREADOR (CÂMARA MUNICIPAL - CRISTÁLIA).
- SRE DE NOVA ERA:
VANIA APARECIDA PEREIRA BASILIO -Masp 1055847-6, EEB(DISP./ADJ.) Ced/Disp/Afast. para exercício de SECRETÁRIO MUNICIPAL DE EDUCAÇÃO(PASSABÉM)/PEB.
- SRE DE PARA DE MINAS:
FABIANA LILIAN BORGES ASSUNCAO -Masp 1273520-5, PEB/PROFESSOR(BOM DESPACHO).
- SRE DE PIRAPORA:
GREYCI GONCALVES RAMOS -Masp 1232890-2, PEB/PROFESSOR(SANTA FÉ DE MINAS).
- SRE DE POCOS DE CALDAS:
JULIO CESAR DE MELO COLABARDINI -Masp 1436773-4, PEB/PROFESSOR(PREFEITURA MUNICIPAL DE ESPIRITO SANTO DO PINHAL - ESTADO DE SÃO PAULO); VANIA BORGES BATISTA DE CARVALHO -Masp 0891403-8, PEB/PROFESSOR(CONCEIÇÃO DA APARECIDA); LETICIA GABRIELLE DE CARVALHO PEREIRA -Masp 1287453-3, PEB/PEB.
- SRE DE POUSO ALEGRE:
MONICA DA CONSOLACAO FREITAS -Masp 0957405-4, PEB/PEB.
- SRE DE SAO JOAO DEL REI:
ADRIANA CRISTINA NEPOMUCENO SILVA -Masp 0665108-7, PEB/PROFESSOR (A) ENSINO FUNDAMENTAL(SÃO JOÃO DEL REI).
- SRE DE TEOFILO OTONI:
ADRIANA FERREIRA DOS SANTOS -Masp 1181668-3, PEB/PEB; ANDREA SOARES NOVAIS BALDRAIA -Masp 1136679-6, PEB/PROFESSOR I(SANTA HELENA DE MINAS); VALNIR MENDES TORRES -Masp 0292112-0, PEB(APOSENTADO)/PEB; MARIA APARECIDA DE SOUZA ALVES -Masp 0640166-5, PEB/PEB; MARIA NATALICE LOPES -Masp 1210140-8, PEB/PROFESSOR I(FRANCISCOPOLIS); REINILDE FERRAZ SANTOS -Masp 1258251-6, PEB/PROFESSOR I(MACHACALIS); MARILDA MARTINS QUARESMA -Masp 0971827-1, PEB(EXERCENDO VICE-DIRECAO)/PEB; CLEITON ALMEIDA DE SOUZA -Masp 1195318-9, PEB/PROFESSOR(PREFEITURA MUNICIPAL DE MUCURI- ESTADO DA BAHIA); FLAVILEIA DA SILVA CRUZ -Masp 1228816-3, PEB/EDUCADOR FÍSICO (PADRE PARAÍSO); EVANILDA CANDIDA DA SILVA MOTA -Masp 0972653-0, ATB/PROFESSOR(LADAINHA); MARINALVA LOPES DA SILVA -Masp 1184963-5, PEB/PEB; MARIA LUCIA TAVARES DE JESUS -Masp 1111845-2, PEB/PROFESSOR(ATALÉIA); DEBORA EDITANIA BARBOSA RAMOS -Masp 1386522-5, PEB/PEB.
- SRE DE UBA:
THIAGO GOMES VIEIRA DA SILVA -Masp 1457159-0, PEB/PROFESSOR(INSTITUTO FEDERAL DO SUDESTE DE MINAS GERAIS); CLEBER LUIS SINGULANI DE SOUZA -Masp 1219493-2, PEB/PEB; EMANUELLE CRISTHYNNE LACERDA GOUVEA -Masp 1194901-3, PEB/PROFESSOR(PIRAÚBA); MARIA AMELIA DE CARVALHO MARTINS -Masp 0869916-7, PEB/PEB; GLEIDE SOARES BALDEZ -Masp 1426385-9, ATB/PROFESSOR(UBÁ); JULIANE OLIVEIRA CAMPOS -Masp 1159903-2, PEB/PEB; DEBORA RIBEIRO DE ALMEIDA -Masp 1359585-5, PEB/PEB; MARIA DO ROSARIO FERREIRA -Masp 1463556-9, PEB/PROFESSOR(PAULA CÂNDIDO); MARISTELA OLIVEIRA LEVINDO -Masp 1303862-5, PEB/PROFESSOR(UBÁ); ANDREIA NALON CORBELLI -Masp 1368716-5, PEB/PEB; MARIA VANDERLEA DE QUEIROZ -Masp 1459743-9, PEB/PEB; ELISABETE DA CONSOLACAO ROBERTO COUTINHO -Masp 0869029-9, EEB/PROFESSOR(PAULA CÂNDIDO); FABIANA DE ARAUJO OLIVEIRA -Masp 0958252-9, PEB/PEB; LETICIA APARECIDA DE LIMA SOARES -Masp 1109090-9, PEB/PEB; BRUNO DA SILVA ARAUJO -Masp 1189453-2, PEB/PEB; NILCEIA BARBOSA DA COSTA -Masp 1145919-5, PEB/PEB; JANEIDE DE FATIMA GONZAGA FORTUNATO -Masp 1176915-5, EEB/PEB; ROSELI DE CASTRO MARTINS PEREIRA -Masp 0866114-2, PEB/PEB.
- SRE DE UBERABA:
ELIANA APARECIDA ALMEIDA OLIVEIRA -Masp 1179799-0, PEB/PROFESSOR(FRUTAL); KENIA DE FATIMA GRACIANO -Masp 1323384-6, PEB/PROFESSOR(FRUTAL); ELENIRIA RODRIGUES DOS SANTOS LEAL -Masp 0973773-5, PEB/PROFESSOR(FRUTAL); SANDRA CRISTINA DE ALCANTARA