Assunto: Portaria
Expediente: 008219-24.00/13-9

PORTARIA Nº. 011/ 2014.

Institui, no âmbito da Secretaria de Estado da Administração e dos Recursos Humanos, o Plano Estratégico de Segurança da Informação - PESI.

O SECRETÁRIO DE ESTADO DA ADMINISTRAÇÃO E DOS RECURSOS HUMANOS, no uso de suas atribuições, em conformidade com o que determina o artigo 35, inciso VI, da Lei n° 13.601, de 01 de janeiro de 2011, e considerando o que prevê as NBR/ISO's 27001 e 27002 e a necessidade de uma plano de segurança da informação,

RESOLVE:

Art. 1° Institui o "Plano Estratégico de Segurança da Informação - PESI", de aplicação no âmbito da Secretaria de Estado da Administração e dos Recursos Humanos - SARH, o qual atenderá às normas estabelecidas no Anexo a esta portaria.
Parágrafo único. As Normas de Segurança da Informação incluídas neste Plano são subdivididas em: Correio Eletrônico, Uso da Internet, Controle de Acesso, Computadores e Recursos Tecnológicos, Dispositivos Móveis e Backup.
Art. 2° O PESI estabelece os regulamentos para a utilização dos recursos tecnológicos no desenvolvimento das atividades de trabalho na SARH.
Art. 3° O PESI estará disponível para consulta e conhecimento no sítio eletrônico (Intranet) da SARH.
Art. 4°. Compete ao Comitê Gestor de Tecnologia da Informação - CGTI, por meio da Divisão de Informática, a atualização das Normas referidas nesta Instrução.
Art. 5° Esta Portaria entra em vigor na data de sua publicação.
Art. 6° Revogam-se as disposições em contrário.

S.A.R.H., em Porto Alegre, 31 de janeiro de 2014.

Codigo: 1274846

ANEXO ÚNICO

Plano Estratégico de Segurança da Informação - PESI

1.0 INTRODUÇÃO

O Plano Estratégico de Segurança da Informação, também referida como PESI, é o documento que orienta e estabelece as normas corporativas da Secretaria da Administração e dos Recursos Humanos para a proteção dos seus ativos de informação.

2.0 TERMOS UTILIZADOS

2.1 SARH: Secretaria da Administração e dos Recursos Humanos.

2.2 DINFO: Divisão de Informática da SARH.

2.3 Ativos de Informação: conjunto de recursos de informática em funcionamento na SARH, envolvendo servidores de rede, estações de trabalho, impressoras, storages e outros equipamentos, além de programas, aplicativos e sistemas utilizados pela SARH.

2.4 Colaborador: toda e qualquer pessoa física (servidor, CC, estagiário, terceirizado, contratado diretamente ou por intermédio de pessoa jurídica, etc.) que tenha acesso a qualquer recurso da rede da SARH

2.5 Gestor: Administrador ou responsável por atividade laboral que utilize recursos da rede da SARH, incluindo pessoas, processos e/ou materiais.

2.6 PESI: Plano Estratégico de Segurança da Informação.

2.7 Download: Recebimento de arquivos pela internet.

2.8 Upload: Envio de arquivos pela internet.

3.0 OBJETIVOS

O objetivo deste documento é de estabelecer normas que garantam aos usuários da rede da SARH seguirem padrões de comportamento alinhados as boas práticas de segurança da informação, bem como, preservar as informações da SARH quanto à:

- **Integridade:** garantir que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantir que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

4.0 APLICAÇÕES DA PESI

As normas aqui estabelecidas são aplicadas a todos os colaboradores da SARH, bem como aos seus prestadores de serviço, e se aplicam à informação produzida na SARH em meio digital. Neste sentido, este plano dá ciência a cada usuário de que os ambientes, sistemas, computadores e redes da SARH poderão ser monitorados, auditados e gravados, conforme previsto nas leis brasileiras.

É obrigação de cada usuário manter-se atualizado em relação a este PESI e aos seus procedimentos e normas relacionadas, buscando orientação do seu gestor ou da DINFO sempre que não estiver absolutamente seguro quanto ao conteúdo descrito.

5.0 PRINCÍPIOS DO PESI

Toda informação produzida ou recebida pelos usuários como resultado da sua atividade profissional pertence à SARH.

Os equipamentos de informática e comunicação, além de sistemas e informações, são utilizados pelos usuários para a realização das suas atividades profissionais.

A SARH, por meio da DINFO, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

6.0 REQUISITOS DA PESI

Para a uniformidade da informação, o PESI deverá ser comunicado a todos os colaboradores da SARH a fim de que suas normas sejam cumpridas dentro e fora da Instituição (situações de utilização de equipamentos móveis).

O PESI deverá ser revisto e atualizado anualmente ou sempre que algum fato relevante ou evento motive sua revisão.

Todo incidente que possa afetar a segurança da informação deverá ser comunicado à DINFO.

O plano de contingência e continuidade do serviço de TI será implantado e testado no mínimo anualmente, visando garantir a segurança da informação.

Conforme a necessidade poderão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a SARH julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à Internet, no correio eletrônico, nos sistemas administrativos e financeiros desenvolvidos pela SARH ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A SARH exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus usuários, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

O não cumprimento do disposto neste PESI acarretará violação às regras internas da Instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

7.0 DAS RESPONSABILIDADES ESPECÍFICAS

7.1 Dos Usuários em Geral

Será de inteira responsabilidade de cada usuário, todo prejuízo ou dano que vier a sofrer ou causar à SARH e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

7.2 Dos Usuários em Regime de Exceção (Temporários e visitantes)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no termo de aceite concedido pela SARH.

A concessão poderá ser revogada a qualquer tempo se for verificada que a justificativa de motivo da atividade não mais compensa o risco relacionado ao regime de exceção ou se o usuário que o recebeu não estiver cumprindo as condições definidas no aceite.

7.3 Dos Gestores

Deverão ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os usuários sob a sua gestão.

7.3.1 Compete aos gestores:

- Atribuir aos usuários sob a sua gestão a responsabilidade pelo cumprimento do PESI da SARH.
- Cadastrar ou descadastrar os colaboradores nos sistemas sob sua responsabilidade e comunicar o seu desligamento e/ou troca de lotação à DIPES para as providências necessárias à atualização nos demais sistemas.

7.4 Da Área de Tecnologia da Informação

7.4.1 Compete à Divisão de Informática:

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por este PESI.
- Gerenciar, junto à PROCERGS, as providências necessárias para a segurança dos sistemas com acesso público.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a SARH.
- Planejar, implantar, fornecer e monitorar as capacidades de armazenamento, processamento e comunicação.
- Proteger continuamente todos os ativos de informação da Instituição contra código malicioso e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da SARH.
- Realizar auditorias periódicas de configurações técnicas e análise de riscos.
- Garantir, da forma mais rápida possível, o bloqueio de acesso de usuários por motivo de desligamento, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da SARH.
- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da SARH.
- Promover a conscientização dos usuários em relação à relevância da segurança da informação para as atividades da SARH, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

8.0 Monitoramento e Auditoria de Ambiente

Para garantir as regras mencionadas neste PESI a SARH poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores de rede, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, sendo a informação gerada por esses sistemas passíveis de serem usadas para a identificação de usuários e seus respectivos acessos;
- Realizar, a qualquer tempo, inspeção física nos equipamentos;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

9.0 CORREIO ELETRÔNICO

O objetivo desta norma é informar aos usuários da SARH quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

9.1 São atividades permitidas quanto ao uso do correio eletrônico:

- A utilização para fins corporativos e em atividades relacionadas à execução dos procedimentos de trabalho;

9.2 São atividades proibidas quanto ao uso do correio eletrônico:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Instituição;
- Enviar mensagem por correio eletrônico pelo endereço de sua lotação ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a SARH ou suas unidades vulneráveis a ações cíveis ou criminais;
- Divulgar informações não autorizadas ou imagens, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

9.2.1 Produzir, transmitir ou divulgar mensagem que:

- Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Vise a obter acesso não autorizado a outro computador, servidor ou rede;
- Vise a interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise a burlar qualquer sistema de segurança;
- Vise a vigiar secretamente ou assediar outro usuário;
- Vise a acessar informações que possam causar prejuízos a qualquer pessoa;
- Tenha conteúdo impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador ou pornográfico;
- Possua conteúdo preconceituoso baseado em orientação sexual, raça, cor, credo, incapacidade física ou mental;
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

10.0 USO DA INTERNET

As regras estabelecidas nesta PESI visam ao desenvolvimento de um comportamento ético e profissional do uso da Internet. Embora a conexão direta e permanente da rede corporativa da SARH com a Internet ofereça um grande potencial de benefícios, ela abre possibilidades para riscos significativos para os ativos de informação.

Essa norma visa à definição das regras de utilização da Internet quanto à navegação a sites e downloads, bem como a uploads de arquivos.

A PROCERGS fará a homologação dos navegadores para a utilização de sistemas/aplicativos utilizados pela SARH (AAP, COE, CFV, SEO, GPE, FPE, SOEWEB, RHE, SGM);

10.1 São procedimentos considerados proibidos na Rede Informatizada da SARH:

- Utilizar os recursos da SARH para fazer download/upload ou distribuição de software ou dados não legalizados;
- Efetuar upload (envio) de qualquer software licenciado à SARH ou de dados de sua propriedade, sem a expressa autorização do responsável pelo software ou pelos dados;
- Divulgar informações confidenciais da SARH em grupos de discussão, listas ou bate-papos;
- Utilizar arquivos que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos;
- Acessar domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos;
- Utilizar softwares de compartilhadores Peer-to-Peer (P2P), tais como Kazaa, Emule, Morpheus, Bitorrent, Ares e afins;
- Acessar, expor, armazenar, distribuir, editar, imprimir ou gravar materiais de cunho sexual por meio de qualquer recurso.
- Utilizar sites que burlam o controle de acesso à internet, tais como Web Proxy.

10.2 O acesso à Internet é divido em 4 (quatro) grupos:

Básico, Intermediário, Avançado e Irrestrito.

	Básico	Intermediário	Avançado	Irrestrito
Download	B	B		
Bancos	B			
Governo				
Órgãos				
Universidades/ Cursos	B			
Comunicação instantânea	B	B		
Streaming	B	B	B	
Relacionamento	B	B	B	
Jogos Online	B	B	B	

B = Bloqueado

O uso da internet será monitorado pela DINFO, mediante ferramentas específicas para aplicação deste plano.

11.0 CONTROLE DE ACESSO

A presente norma visa a estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os usuários.

Os dispositivos de identificação e senhas protegem a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a SARH e/ou terceiros.

Sendo a DIPES (Divisão de Pessoal da SARH) responsável pelo ingresso dos servidores e estagiários, cabe à mesma solicitar a criação de login, e-mail e usuário SOEWEB, informando o local de lotação do servidor ou estagiário, bem como informar os desligamentos, para que a DINFO providencie o bloqueio de acesso.

Nas situações de troca de lotação de colaboradores a DIPES deverá comunicar a DINFO para que essa providencie as alterações necessárias nos sistemas informatizados.

O compartilhamento de login é proibido para quaisquer atividades.

É de responsabilidade de cada colaborador a utilização de sua própria senha, sendo ela pessoal e intransferível.

Os usuários podem alterar a própria senha, devendo fazê-lo caso suspeitem que terceiros tenham obtido conhecimento indevido.

Caso o usuário esqueça sua senha, deverá requisitar formalmente a sua alteração à DINFO.

12.0 COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos usuários são de propriedade da SARH, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas chefias responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação sem o conhecimento prévio e o acompanhamento de um técnico da DINFO ou de quem esta determinar.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida homologação da DINFO e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter o software antivírus adotado pela SARH instalado, ativado e atualizado permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a DINFO mediante registro de chamado ou email.

Os arquivos pessoais e/ou não pertinentes às atividades da SARH (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois sobrecarregarão o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles serão excluídos.

Documentos pertinentes e imprescindíveis para as atividades de cada usuário da SARH deverão ser salvos nos seguintes locais:

Unidade U: (<setor>)	Armazenar arquivos pertinentes às atividades do setor ao qual o colaborador está lotado. A responsabilidade de manutenção é do próprio setor.
Unidade S: (<setor-siarq>)	Classificar e armazenar documentos, eletronicamente, de acordo com as normas do SIARQ(Sistema de Arquivos).

Os arquivos gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

12.1 Regras para o uso dos computadores, equipamentos e recursos de informática:

- Os usuários devem informar à DINFO qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio para qualquer tipo de reparo que não seja realizado por um técnico da DINFO ou por terceiros devidamente contratados para o serviço.
- É expressamente proibido o consumo de alimentos e bebidas próximo aos equipamentos.
- Deverão ser protegidos por senha (bloqueados), todos os terminais de computador quando não estiverem sendo utilizados.

12.2 Proibições quanto ao uso de computadores e recursos tecnológicos da SARH:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método lícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software sem as devidas licenças do fabricante ou detentor dos direitos (comumente chamado de pirata).

13.0 DISPOSITIVOS MÓVEIS

Para fins deste PESI, entende-se por "dispositivo móvel" qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da Instituição ou de terceiros, desde que aprovado e permitido pela DINFO, como: notebooks, smartphones, pendrives, tablets etc.

Essa norma visa a estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os usuários que utilizem tais equipamentos.

O usuário assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na SARH, mesmo depois de terminado o vínculo mantido com a instituição.

A SARH reserva-se o direito de inspecionar os equipamentos de sua propriedade a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O suporte técnico dos dispositivos móveis de propriedade da SARH deverá seguir o mesmo fluxo de suporte adotado pela Instituição para os demais equipamentos da rede.

Todos os usuários deverão utilizar senhas de bloqueio automático para os dispositivos móveis.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da DINFO e sem a condução, auxílio ou presença de um de seus técnicos.

O usuário será o único responsável por manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da DINFO.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela Instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

A utilização de rede banda larga de locais conhecidos pelo usuário, como sua casa, hotéis e fornecedores é permitida.

O uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o usuário o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha a causar à SARH e/ou a terceiros.

O usuário é responsável por todos os acessórios que acompanham ou fazem parte dos dispositivos móveis, devendo mantê-los sempre junto aos mesmos.

14.0 BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento e serão executados após o término do expediente, nas chamadas "janelas de backup" (a partir das 21h) - períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

As mídias de backup serão acondicionadas em local seco, climatizado, seguro (cofres corta-fogo segundo as normas da ABNT) e em local distante do CAFF.

As operações de restauração de arquivos serão efetuadas num prazo máximo de 48 horas do registro da solicitação do serviço, tempo este necessário para a busca nos dispositivos de mídia armazenados em local diverso da sede da SARH.

As solicitações de restauração de arquivo devem conter: nome de arquivos, pasta de armazenamento e a provável data de exclusão.

Somente serão passíveis de restauração os arquivos pertinentes ao serviço e que estejam salvos na unidade de rede "U".

15.0 DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da SARH. Ou seja, qualquer incidente de segurança subentende-se como alguém agindo contra a ética e os bons costumes regidos pela Instituição.

Codigo: 1274847

DEPARTAMENTO DE ADMINISTRAÇÃO DO PATRIMÔNIO DO ESTADO

PORTARIA Nº 217/2013

O Secretário da Administração e dos Recursos Humanos, no uso da atribuição que lhe é conferida pelo artigo 6º, inciso XVII, do Decreto Nº 47.715, de 28 de dezembro de 2010, **DESIGNA** os servidores **Maiquel Fernando de Sousa Póvoa**, Identificação Funcional no Sistema de Recursos Humanos do Estado nº 3495620/01 , **Cleber Daunis Praça**, Identificação Funcional no Sistema de Recursos Humanos do Estado nº 3780902/01 ou **Hélio Soares dos Santos**, Identificação Funcional no Sistema de Recursos Humanos do Estado nº 1422103/01, para representar o Estado do Rio Grande do Sul na assinatura da **ESCRITURA PÚBLICA DE AQUISIÇÃO DE IMÓVEL**, no Município de São Francisco de Paula/RS, em conformidade com o contido no processo administrativo nº **005643-05.00/13-6**.

Secretaria da Administração e dos Recursos Humanos, em Porto Alegre, ____ / ____ / _____.

Alessandro Pires Barcellos
SECRETARIA DA ADMINISTRAÇÃO E DOS RECURSOS HUMANOS

Registre-se e publique-se.

Codigo: 1274844

PATRIMÔNIO

Assunto: DESTINAÇÃO DE USO
Expediente nº 007394-2400/09-2
Termo de DESTINAÇÃO DE USO celebrado pelo Estado Rio Grande do Sul, relativo ao imóvel lançado no DEAPE/SARH sob o nº 23830, nas condições a seguir:
ÓRGÃO: TRIBUNAL DE JUSTIÇA;
USUÁRIO: CONSTRUÇÃO DE NOVO FÓRUM;
OBJETO: Terreno com área de 1.125,0000m²;
FINALIDADE: FÓRUM;
DATA DE INÍCIO: 22/09/2009.

Codigo: 1274848

RECURSOS HUMANOS

Assunto: Gratificação por Risco de Vida
Expediente: 109978-1900/13-6
Nome: Catia Maria Armelin Peruzzo
Id.Func./Vínculo: 2387538/01
Tipo Vínculo: efetivo
Cargo/Função: Professor - B-6
Lotação: SEDUC - 16 Coordenadoria Regional de Educação

CONCEDE Gratificação por risco de vida de 45%, a servidora em exercício pelo atendimento a sala de recursos no Instituto Estadual de Educação Tiradentes, face convocação, a contar de 29/10/2012 a 31/12/2012, conforme laudo da DISAT 0086/2014, no regime de trabalho de 10 horas semanais, nos termos da Lei 8704/88, art. 1º com a redação alterada pela Lei 9889/93 e Lei 8804/89.

Codigo: 1274849

Assunto: Gratificação por Risco de Vida
Expediente: 002660-2000/14-2
Nome: Jacinda Lehmen Stahl
Id.Func./Vínculo: 3534227/01
Tipo Vínculo: comissionado
Cargo/Função: Chefe de Divisão - CC10
Lotação: Secretaria da Saúde

CONCEDE Gratificação por risco de vida de 45%, a servidora em exercício no Hospital Sanatório Partenon, a contar de 06/11/2013, conforme laudo da DISAT 0087/2014, nos termos da Lei 8704/88, art. 1º com a redação alterada pela Lei 9889/93.

Codigo: 1274850

Assunto: Gratificação por Risco de Vida
Expediente: 058214-1900/13-6
Nome: Maria Cristina Miritz Silva
Id.Func./Vínculo: 2472295/01
Tipo Vínculo: efetivo
Cargo/Função: Professor - A-6
Lotação: SEDUC - 05 Coordenadoria Regional de Educação

CONCEDE Gratificação por risco de vida de 45%, a servidora em exercício pelo atendimento a sala de recursos na Colégio Estadual Cassiano do Nascimento, face provimento, a contar de 13/11/2012, conforme laudo da DISAT 0081/2014, no regime de trabalho de 20 horas semanais, nos termos da Lei 8704/88, art. 1º com a redação alterada pela Lei 9889/93 e Lei 8804/89.

Codigo: 1274851