

PORTARIA Nº. 293/GARH/GAB/IPERON, DE 11 DE MAIO DE 2015.

Designar servidor.

A PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO ESTADO DE RONDÔNIA no uso de suas atribuições que lhe confere o Decreto de 15 de janeiro de 2015;

Considerando as atribuições definidas no Decreto nº 13.627, de 21/05/2008, especificamente o Artigo 8º, inciso XIX;

RESOLVE:

Art. 1º **DESIGNAR** o servidor JOÃO CELINO DURGO SANTOS NETO, matrícula 300040511, para responder pelo expediente da Diretoria de Previdência, em substituição a UNIVERSA LAGOS, no período de 13 a 15/05/2015, por motivo de participação na 53ª Reunião Ordinária do Conselho Nacional dos dirigentes de RPPS – CONAPREV, que será realizado na cidade de Brasília-DF.

Art. 2º. Encaminhe-se cópia desta portaria para publicação, bem como anotações nos apontamentos funcionais da servidora.

Registre-se.Cumpra-se.

MARIA REJANE SAMPAIO DOS SANTOS VIEIRA
Presidente do IPERON

PORTARIA Nº. 294/GARH/GAB/IPERON, DE 11 DE MAIO DE 2015.

Conceder afastamento remunerado.

A PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO ESTADO DE RONDÔNIA no uso de suas atribuições que lhe confere o Decreto de 15 de janeiro de 2015;

Considerando as atribuições definidas no Decreto nº 13.627, de 21/05/2008, especificamente o Artigo 8º, inciso XIX;

Considerando o teor do Processo 01-1320.00350-0000/2015, Cota às fls. 21 verso da Procuradoria Geral/IPERON.

RESOLVE:

Art. 1º. **CONCEDER** afastamento remunerado para aguardar homologação de aposentadoria a partir de 13/05/2015, com base no Art. 13 da Lei Complementar 1068/2002, à servidora **MARIA RILDA DA SILVA LOYO**, Administrador, matrícula 300037381, pertencente ao Quadro de Pessoal do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON.

Art. 2º. Encaminhe-se cópia desta portaria para publicação, bem como anotações nos apontamentos funcionais da servidora.

Registre-se.Cumpra-se.

MARIA REJANE SAMPAIO DOS SANTOS VIEIRA
Presidente do IPERON

PORTARIA Nº. 297/GARH/GAB/IPERON, DE 08 DE MAIO DE 2015

Nomear Comissão para gestão de contratos.

A PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO ESTADO DE RONDÔNIA no uso de suas atribuições que lhe confere o Decreto de 15 de janeiro de 2015;

Considerando as atribuições definidas no Decreto nº 13.627, de 21/05/2008, especificamente o Artigo 8º, inciso XIX;

RESOLVE:

Art. 1º. **NOMEAR** a Comissão encarregada para fiscalizar, certificar e emitir Termo de Recebimento de Serviços, conforme prevê a Lei nº 8666, Artigos 67 e 73, Inciso I, alínea I, combinado com o Art. 63 da Lei 4320/64, em conformidade com o Contrato de nº 001/2015/IPERON, Processo nº 01-2220.01871-0000/2014, tendo como objeto serviços de vigilância armada, diurna e noturna, visando atender ao Instituto de Previdência dos Servidores Públicos do Estado de Rondônia.

Gestor do Contrato:

Antônio de Almeida Silva
Técnico em Previdência
Matrícula nº 300031372

Membros:

Alba Solange Ferreira dos Santos Guimarães
Gerente de Administração e Recursos Humanos
Matrícula nº 300130602

Leidimar Raimunda Nunes de Lima
Técnico em Previdência
Matrícula nº 300031412

Laésio de Lima Leite

Preposto da Empresa FBX Serviços de Segurança Ltda.
RG nº 4026895 SSP/RO

Art. 2º. São atribuições do Gestor do Contrato:

- acompanhar os prazos de execução dos serviços, diligenciando com a empresa contratada, se necessário;
- receber, provisória e definitivamente, os serviços sob sua responsabilidade;
- analisar, conferir e atestar notas fiscais, faturas e congêneres e a regularidade fiscal do contratado;
- devolver à contratada as notas fiscais em desconformidade com o Contrato;
- controlar prazos de vigência dos instrumentos contratuais sob sua responsabilidade, solicitando sua prorrogação, realização de licitação ou contratação direta, conforme o caso;
- informar ao Ordenador de Despesas, nos respectivos autos ou por meio de Comunicação Interna, o interesse na prorrogação dos contratos sob sua responsabilidade, visando à obtenção da competente autorização;
- oficiar à contratada determinação de medidas preventivas e corretivas, com estabelecimento de prazos, para regularização das faltas registradas e/ou defeitos observados na execução do contrato;
- informar à Administração, nos autos, o não atendimento à determinação de que trata o inciso anterior, pronunciando-se quanto às justificativas apresentadas pela contratada;
- manter controle atualizado dos pagamentos;
- manifestar-se em todos os atos da Administração relativos à aplicação de penalidades, execução, alteração, reajuste e repactuação dos contratos;
- participar, obrigatoriamente, de negociações contratuais;
- autorizar, formalmente, quando do término da vigência do contrato, a liberação da garantia contratual em favor da contratada, se houver;
- diligenciar e zelar pela fiel execução do objeto contratado, com vista a salvaguardar os interesses do Estado, bem como observar o estrito cumprimento da legislação que regulamenta a matéria.

Art. 3º. É competência da Comissão acompanhar, averiguar, emitir relatórios e documentos que subsidiem a correta prestação dos serviços contratados.

Art. 4º. Na ausência e impedimentos dos mesmos, ficarão responsáveis por certificar e emitir relatório conforme descrito no art. 1º, os seus substitutos legais.

Art. 5º. Esta Portaria entrará em vigor a contar desta data.

Art. 6º. Encaminhe-se cópia desta portaria para publicação, bem como anotações nos apontamentos funcionais dos servidores.

Registre-se.Cumpra-se.

MARIA REJANE SAMPAIO DOS SANTOS VIEIRA
Presidente do IPERON

RESOLUÇÃO NORMATIVA Nº. 001/GAB/IPERON, DE 30 DE ABRIL DE 2015.

Dispõe sobre a Política Corporativa de Segurança da Informação do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON (PCSI/ IPERON).

A PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO ESTADO DE RONDÔNIA no uso de suas atribuições que lhe confere o Decreto de 15 de janeiro de 2015;

CONSIDERANDO as atribuições definidas no Decreto nº 13.627, de 21/05/2008, especificamente o Artigo 8º, inciso XIX;

Considerando que o IPERON gera, adquire ou absorve informações no exercício de suas competências constitucionais, legais e regulamentares, e que essas informações devem permanecer íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

Considerando que as informações no IPERON são armazenadas em diferentes suportes, veiculadas por diferentes formas, tais como meio impresso, eletrônico e microforma, e, portanto, vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

Considerando que a adequada gestão da informação precisa nortear todos os processos de trabalho e unidades do IPERON e deve ser impulsionada pela Política Corporativa de Segurança da Informação;

Considerando que a NBR ISO/IEC 27002:2005, norma que estabelece boas práticas em segurança da informação, recomenda revisões periódicas da política de segurança da informação das instituições;

RESOLVE:

Art. 1º. Instituir a Política Corporativa de Segurança da Informação do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia (PCSI/IPERON) que observará os princípios, objetivos e diretrizes estabelecidos nesta Resolução, bem como as disposições constitucionais, legais e regimentais vigentes.

CAPÍTULO I DO CONCEITO

Seção I Das Disposições Gerais

Art. 2º. A PCSI/IPERON alinha-se às estratégias do Instituto e tem por objetivo garantir a autenticidade, a confidencialidade, a disponibilidade e a integridade das informações produzidas ou custodiadas pelo IPERON.

Art. 3º. Para os efeitos desta Resolução, entende-se por:

I - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

II - Segurança da informação: proteção da informação contra ameaças para garantir sua continuidade, minimizar os riscos e maximizar a eficiência e a efetividade das ações do negócio;

III - Gestor da informação: unidade ou projeto do IPERON que, no exercício de suas competências, produz ou obtém, de fonte externa ao Instituto, informações de propriedade de pessoa física ou jurídica;

IV - Custodiante: pessoa física, unidade ou projeto do IPERON que detém a posse, mesmo que transitória, de informação produzida ou recebida pelo Instituto;

V - Incidente em segurança da informação: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações ou ameaçar a segurança da informação.

Seção II Dos Princípios

Art. 4º. A segurança da informação no IPERON abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos seguintes Princípios:

I - Confidencialidade: garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;

II – Disponibilidade: garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;

III - Integridade: garante a não-violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital.

Art. 5º. São Princípios da PCSI/IPERON:

I - Toda informação produzida ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, pertence ao IPERON. As exceções devem ser explícitas e formalizadas entre as partes;

II - Todos os recursos de informação do IPERON devem ser projetados para que seu uso seja consciente e responsável. Os recursos comunicacionais e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finalísticos;

III - Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a Instituição julgar necessário, com vistas à redução dos riscos dos seus ativos de informação;

IV - Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários (privilegios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade;

V - Todo o acesso a redes e sistemas do Instituto deverá ser feito, preferencialmente, por meio de login de acesso único, pessoal e intransferível;

VI - O IPERON pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada na infraestrutura provida pelo Instituto;

VII - Cada usuário é responsável pela segurança das informações dentro do IPERON, principalmente daquelas que estão sob sua responsabilidade;

VIII - Esta Política Corporativa de Segurança da Informação será implementada no IPERON por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

Seção III Dos Objetivos e Perfil

Art. 6º. Para os efeitos desta Resolução, os Objetivos da PCSI/IPERON, além de buscar preservar as informações, são:

I - Estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional;

II - Designar, definir ou alterar papéis e responsabilidades do grupo responsável pela Segurança da Informação;

III - Apoiar a implantação das iniciativas relativas à Segurança da Informação;

IV - Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

Art. 7º. Os papéis e perfis a serem executados no PCSI/IPERON consistem na definição contida na Tabela 1:

Tabela 1: Descrição de papéis em Segurança da Informação

Tabela 1: Descrição de papéis em Segurança da Informação		
PAPEL	PERFIL ASSOCIADO	DESCRIÇÃO
USUÁRIO INTERNO	Servidores públicos, servidores sem vínculo, demais funcionários e colaboradores internos.	Todos os servidores, gestores, técnicos, estagiários, bolsistas de programas educacionais, consultores e colaboradores internos, que fazem uso dos recursos informacionais e computacionais do IPERON.
USUÁRIO EXTERNO	Prestadores de serviço e demais colaboradores externos.	Prestadores de serviços contratados direta ou indiretamente pela IPERON e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais.
GESTORES	Coordenadores, Diretores, Gerentes e demais cargos de chefia.	Todos aqueles que exercem funções de chefia no âmbito do IPERON, administrando pessoas e/ou processos.
ÁREA DE TI	Coordenadoria de Sistema (COOSIST)	Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e custo diante da informação.

**CAPÍTULO II
DAS RESPONSABILIDADES
Seção I**

Responsabilidades Gerais

Art. 8º. As responsabilidades gerais na PCSI/IPERON são de todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais do IPERON e incluem:

I - Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso;

II - Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do Instituto;

III - Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do IPERON;

IV - Manter-se atualizado em relação a esta PCSI e às normas e procedimentos relacionados, buscando informação junto ao Gestor de Segurança da Informação da Instituição sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações.

**Seção II
Responsabilidades Específicas**

Art. 9º. As responsabilidades específicas são definidas de acordo com o perfil estabelecido:

I - Usuários internos e externos:

Será de inteira responsabilidade de cada usuário (interno ou externo) todo prejuízo ou dano que vier a sofrer ou causar ao IPERON em decorrência da não obediência às diretrizes e normas referidas na PCSI/IPERON e nas normas e procedimentos específicos dela decorrentes.

Os usuários externos devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes. O IPERON poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da PCSI/IPERON ou das normas e procedimentos específicos dela decorrentes.

II - Gestores de pessoas e processos:

Os gestores executivos do IPERON devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão.

Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação do IPERON, tomando as ações necessárias para cumprir tal responsabilidade.

III - Gestores e usuários da Área de Tecnologia da Informação:

a) Zelar pela eficácia dos controles de Sistemas da Informação utilizados e informar aos gestores e demais interessados os riscos residuais;

b) Negociar e acordar com os gestores níveis de serviço relacionados a Sistemas da Informação, incluindo os procedimentos de resposta a incidentes;

c) Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

d) Zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e eliminar a existência de pessoas que possam excluir logs e trilhas de auditoria das suas próprias ações;

e) Implantar controles que gerem registros auditáveis para retirada e transporte de mídias que contenham informações custodiadas pela TI, nos ambientes totalmente controlados por ela;

f) Informar previamente ao Gestor de Sistemas da Informação sobre o fim do prazo de retenção de informações, para que este tenha a alternativa de alterá-lo ou postergá-lo, antes que a informação seja definitivamente descartada pelo custodiante;

g) Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a uma pessoa física identificável como responsável pelo uso da conta (a responsabilidade pela gestão dos logins de usuários externos é do gestor do contrato de prestação de serviços ou do gestor do setor em que o usuário externo desempenha suas atividades);

h) Proteger continuamente todos os ativos de informação do Instituto contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código mal-intencionado e/ou indesejado;

i) Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção do IPERON ou em fase de mudança de ambiente de desenvolvimento, teste, homologação ou produção de sistemas (quando tais ambientes forem acessados por terceiros, a responsabilização deve ser explicitada nas cláusulas dos instrumentos contratuais);

j) Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional e/ou dedicados à visitação externa, exigindo o seu cumprimento dentro da Autarquia;

k) Garantir, da forma mais rápida possível, com recebimento de solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento do IPERON, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos do instituto.

**CAPÍTULO III
AS DIRETRIZES**

**Seção I
Das Diretrizes Gerais**

Art. 10. Ficam definidas as diretrizes específicas e procedimentos próprios de tratamento da informação corporativa, as quais adotarão as seguintes diretrizes gerais:

I - A informação utilizada pelo IPERON é um bem que tem valor. Ela deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, autenticidade e auditabilidade, independente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado;

II - Documentos imprescindíveis para as atividades dos usuários da Instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário;

III - Arquivos pessoais e/ou não pertinentes às atividades institucionais do IPERON (fotos, músicas, vídeos, etc..) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificado, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário;

IV - Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação dessa Norma;

V - O acesso da informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Esse acesso acontece através da identificação e autenticação do usuário;

VI - O ambiente do sistema computacional destinado à execução dos sistemas e o ambiente de produção não devem ser utilizados para testes. Os testes devem ser feitos em recinto apropriado e gerenciado;

VII - A passagem de programas e dados para o ambiente de produção deve ser controlada de maneira a garantir a integridade e disponibilidade desse recinto para sua execução;

VIII - Todos os procedimentos que possibilitam a proteção da informação e a continuidade de seu uso devem ser documentados, de tal forma que possibilite que a organização continue a operacionalização desses procedimentos;

IX - Devem ser estabelecidos critérios para deleções seguras de informações armazenadas em estações de trabalho e/ou outros dispositivos de armazenamento, como formatação de máquinas ou desmagnetização de discos, quando o equipamento for transferido para outro usuário ou descartado pelo IPERON para algum outro destino;

X - O Gestor da Informação é a pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação;

XI - A destruição de dados sigilosos deve ser feita por método que sobrescreva as informações armazenadas. Se não estiver ao alcance do Órgão a destruição lógica, deverá ser providenciada a destruição física por incineração dos dispositivos de armazenamento;

XII - Toda informação crítica para o funcionamento do IPERON deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção adequada. O Gestor da Informação é responsável pela definição dessa criticidade.

Seção II Das Diretrizes Específicas

Art. 11. As Diretrizes Específicas deverão seguir as seguintes normativas:

§ 1º. Fica estabelecido o controle de acesso físico e lógico no ambiente computacional do IPERON:

I - Dos Controles de Acesso Físico:

a) Os controles de acesso físico visam restringir o acesso aos equipamentos, documentos e suprimentos do IPERON e à proteção dos recursos computacionais, permitido apenas às pessoas autorizadas;

b) Devem ser adotados controles que restrinjam a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança e habilitando o acesso apenas de pessoal autorizado. No caso de sistemas críticos, convém que sejam criados ambientes reservados, de uso exclusivo, para abrigá-los;

c) Todo o pessoal envolvido em trabalhos de apoio tais como a manutenção das instalações físicas, deve ser orientado e capacitado para manter a adoção de medidas de proteção ao acesso;

d) Todas as pessoas devem portar algum tipo de identificação visível que informe se é um servidor ou não, bem como o nível de autorização de acesso;

e) O ingresso de visitantes deve ser controlado de tal forma a impedir o acesso destes às áreas de armazenamento ou processamento de informações sensíveis, salvo acompanhados e com autorização do responsável.

II - Dos Controles de Acesso Lógico:

a) Os controles de acesso lógico são um conjunto de procedimentos, recursos e meios utilizados com a finalidade de prevenir e/ou obstruir ações de qualquer natureza que possam comprometer recursos computacionais, redes corporativas, aplicações e sistemas de informação;

b) Os trechos que abrigam meios de comunicação devem ser protegidos para evitar a interceptação e/ou interferência de dados;

c) Os computadores e sistemas do IPERON devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado;

d) Os sistemas devem ser avaliados com relação aos aspectos de segurança antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas;

e) O acesso remoto aos recursos computacionais deve ser realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço;

f) O Suporte Técnico do IPERON poderá ter permissão de acesso remoto às estações de trabalho dos usuários das unidades quando necessário.

§ 2º. Ficam estabelecidos critérios para a disponibilização e administração do

acesso aos serviços de tecnologia de informação do IPERON, assim como estabelecer critérios relativos às senhas das respectivas contas.

I - O controle de acesso deverá considerar e respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação do IPERON;

II - A criação e administração de contas serão realizadas de acordo com procedimento específico para todo e qualquer usuário. Para o usuário que não exerce funções de administração de rede será privilegiada a criação de uma única conta institucional de acesso, pessoal e intransferível. Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação;

III - O acesso à rede corporativa deve dar-se de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em norma específica;

IV – da criação da Conta de Acesso:

a) Todo cadastramento de conta de acesso à rede do IPERON deve ser efetuado mediante solicitação formal;

b) Contas de acesso de terceirizados do IPERON devem ter prazo de validade no máximo igual ao período de vigência do contrato ou período de duração de suas atividades;

c) As solicitações relativas à criação de cada conta devem ser registradas e armazenadas de forma segura pela COOSIST/IPERON;

d) Todos os usuários devem assinar Termo de Responsabilidade pela utilização da conta de acesso, ao qual deverá ser entregue junto com a solicitação de criação da conta de acesso;

e) A nomenclatura das contas de acesso de usuários deve seguir padrão definido pela COOSIST/IPERON;

f) A chefia imediata da área a qual pertence o usuário deve ser informada formalmente, pela COOSIST/IPERON, a respeito de qualquer evento relacionado a falhas de segurança referente à conta do usuário e senha;

g) Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada à COOSIST/IPERON.

V – da exclusão e bloqueio da Conta de Acesso

a) Toda exclusão ou bloqueio de conta de acesso à rede do IPERON deve ser efetuado mediante solicitação formal;

b) A exclusão da conta de acesso do usuário deve ser solicitada caso haja:

- Falecimento;
- Aposentadoria; e
- Outros afastamentos que caracterizem encerramento do vínculo com a instituição;

c) Contas sem utilização por mais de 45 (quarenta e cinco) dias serão bloqueadas;

d) As contas deverão permanecer bloqueadas até que haja nova solicitação formal para desbloqueio;

e) As contas de serviços utilizadas em servidores de rede, backup, correio eletrônico, banco de dados, aplicações, entre outros, devem ser utilizadas somente para execução de ações ligadas à sua natureza, de forma automática, sem intervenção manual através de logon/acesso;

f) As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas, em equipamentos previamente definidos. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede e chefia respectiva.

VI - das Senhas

- a) Todas as senhas, de usuários comuns, para autenticação na rede do IPERON devem seguir os seguintes critérios mínimos:
- b) Toda senha deve ser constituída de, no mínimo, 8 caracteres sendo obrigatório o uso de caracteres alfanuméricos (letras e números);
- c) A senha não poderá conter parte do nome do usuário, por exemplo: se o usuário chama-se Jose da Silva, sua senha não pode conter partes do nome como "1221jose" ou "1212silv";
- d) A data de expiração da senha deve ser de no máximo 90 dias, caso não seja alterada, esta será bloqueada;
- e) É obrigatória a troca de senha ao efetuar o primeiro login;
- f) É proibida a repetição das 5 últimas senhas já utilizadas;
- g) Os critérios definidos acima serão auditados pela COOSIST/IPERON, por meio de ferramentas adequadas;
- h) A base de dados de senhas deve ser armazenada com criptografia;
- i) O usuário poderá solicitar alteração de sua senha, caso não se recorde da mesma, mediante solicitação formal;

VII - da Utilização de Contas de Acesso e Senhas

- a) A conta de acesso é o instrumento para identificação do usuário na rede IPERON e caracteriza-se por ser de uso individual e intransferível e sua divulgação é vedada sob qualquer hipótese;
- b) Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário, ao qual as informações estão vinculadas;
- c) A Diretoria Administrativa e Financeira do IPERON deve comunicar à COOSIST/IPERON, no prazo de dois dias úteis, os desligamentos, as aposentadorias, os afastamentos e as movimentações de usuários que impliquem mudanças de lotação;
- d) O acesso aos serviços de tecnologia de informação do IPERON deve ser disponibilizado aos membros, servidores, estagiários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do IPERON;
- e) Para fins de auditoria, as contas de administradores locais das estações de trabalho ou de servidores de rede só devem ser utilizadas quando estritamente necessário.

§ 3º. Fica instituído aos colaboradores do IPERON, os serviços de correio eletrônico (e-mail):

I - O correio eletrônico é uma ferramenta disponível e obrigatória para todos os usuários do IPERON, independentemente de seu vínculo funcional;

II - O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais do IPERON;

III - São usuários do serviço de correio eletrônico corporativo os membros e servidores do IPERON, seus órgãos e unidades, os estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional do IPERON;

IV - A concessão de contas de correio eletrônico depende de pedido fundamentado da autoridade responsável pela respectiva área, demonstrando a necessidade, para a Instituição, da utilização do serviço pelo agente;

V - Os titulares de órgão ou unidade do IPERON podem solicitar a criação de listas de distribuição, restritas aos seus respectivos âmbitos de atuação;

VI - Cada unidade do IPERON manterá no mínimo uma conta de correio eletrônico, destinada a comunicações institucionais;

VII - É vedado o acesso ao conteúdo das mensagens tramitadas por meio do serviço de correio eletrônico corporativo, salvo nas hipóteses previstas em lei;

VIII - O acesso indevido às informações tramitadas por meio do serviço de correio eletrônico corporativo do IPERON, ou contidas em seus ambientes, será punido na forma da Lei;

IX - O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação;

X - É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:

- Praticar crimes e infrações de qualquer natureza;
- Executar ações nocivas contra outros recursos computacionais do IPERON ou de redes externas;
- Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;
- Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo "corrente", vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede do IPERON;
- Emitir comunicados gerais com caráter eminentemente associativo, sindical ou político-partidário;
- Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pelo IPERON;
- Divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço;
- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento 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 o IPERON ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, 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, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do IPERON estiver sujeita a algum tipo de investigação;
- Fornecer orientação que conflite ou contrarie os interesses do IPERON;
- Disseminar ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- Distribuir ou fazer uso de 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;
- Obter acesso não autorizado a outro computador, servidor ou rede;
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Burlar qualquer sistema de segurança;
- Vigiar secretamente ou assediar outro usuário;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

- Incluir imagens criptografadas ou de qualquer forma mascaradas;
- Distribuir conteúdo considerado impróprio, obsceno ou ilegal, de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Distribuir conteúdo de perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Distribuir conteúdo que tenha fins políticos locais ou do país (propaganda política);
- Incluir material protegido por direitos autorais sem a permissão do detentor dos direitos;
- Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

§ 4º. Fica estabelecido procedimentos de controle de uso e acesso à Internet no âmbito do IPERON:

- a) Todas as regras corporativas sobre uso de Internet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, a proteção dos ativos de informação do IPERON deverá sempre ser privilegiada;
- b) Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos ocupantes de cargo efetivo. Quando não for possível, a equipe pode ser mista, desde que sob a coordenação e responsabilidade de um servidor do quadro permanente do órgão;
- c) Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, o IPERON, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à rede mundial de computadores;
- d) Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, sítio, caixa postal de correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando a assegurar o cumprimento da PCSI/IPERON;
- e) Os colaboradores com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades do IPERON e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelo Setor de Informática;
- f) É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

CAPÍTULO IV DAS PENALIDADES

Seção I Penalidades

Art. 12. O não cumprimento das determinações ora apresentadas sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos do IPERON;

§ 1º. O descumprimento das disposições constantes nessa PCSI/IPERON sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil;

§ 2º. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na Lei Complementar nº 68/92 e demais legislação pertinente;

CAPÍTULO VI DA ATUALIZAÇÃO

Seção I Atualização

Art. 13. Esse PCSI/IPERON deve ser revisada e atualizada periodicamente no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

Art. 14. As informações produzidas por usuários do IPERON e não cabe a seus criadores qualquer forma de direito autoral.

§ 1º. Quando as informações forem produzidas por terceiros para uso exclusivo do IPERON, instrumento próprio obrigará os criadores ao sigilo permanente do conteúdo dos produtos.

§ 2º. É vedada a utilização das informações a que se refere o parágrafo anterior em quaisquer outros projetos ou atividades de uso diverso ao estabelecido pelo IPERON, salvo autorização específica pela Presidência, nos processos e documentos de sua competência e demais casos.

CAPÍTULO VII DAS DISPOSIÇÕES FINAIS

Art. 15. Para a uniformização da informação organizacional, esta PCSI/IPERON deverá ser comunicada a todos os gestores, servidores, colaboradores e prestadores de serviço do IPERON – a fim de que seja cumprida dentro e fora da autarquia.

Art. 16. O não cumprimento dos requisitos previstos nesta política, nas normas complementares e nos procedimentos de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

Art. 17. Os casos omissos e as dúvidas surgidas na aplicação dessa política serão submetidos a Procuradoria Geral e Presidência do IPERON;

Art. 18. Esta Resolução entra em vigor na data de sua publicação.

MARIA REJANE SAMPAIO DOS SANTOS VIEIRA
Presidente do IPERON

AVISO DE INEXIGIBILIDADE DE LICITAÇÃO

A PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO ESTADO DE RONDÔNIA - IPERON torna público a quem possa interessar, que nos termos do art. 25, inciso II, da Lei Federal nº. 8.666/93, nos autos do Processo Administrativo nº 01-1320.00426-0000/2015, objetivando a contratação de empresa especializada na prestação de serviços em treinamento de agentes públicos, em favor de **BRASIL FORTE SOLUÇÕES EM SERVIÇOS LTDA-ME**, inscrito no CNPJ nº 14.395.182/0001-51, no valor de R\$ 2.960,00 (dois mil, novecentos e sessenta reais) conforme INFORMAÇÃO nº 635/2015/PGE/IPERON, de 30.04.2015, acostado às fls. 29/33 dos autos em epígrafe. Porto Velho (RO), 04 de maio de 2015.

Maria Rejane Sampaio dos Santos Vieira
Presidente do IPERON

TERMO DE RATIFICAÇÃO

RATIFICO a despesa no valor total de R\$ 2.960,00 (dois mil, novecentos e sessenta reais), conforme INFORMAÇÃO nº 635/2015/PGE/IPERON, de acordo com o disposto no art. 25, inciso II, da Lei Federal nº 8.666/93. Porto Velho (RO), 04 de maio de 2015.

Maria Rejane Sampaio dos Santos Vieira
Presidente do IPERON