b) a comprovação pelo proponente de projeto desportivo aprovado, das respectivas regularidades fiscais e tributárias nas esferas federal, estadual e municipal, nos termos do parágrafo único do art. 27 do Decreto nº 6.180 de 3 de agosto de 2007 decide:

Art. 1º Tornar pública, para os efeitos da Lei nº 11.438 de 2006 e do Decreto nº 6.180 de 2007, a aprovação dos projetos desportivos relacionados no anexo I.

Art. 2º Autorizar a captação de recursos, nos termos e prazos expressos, mediante doações ou patrocínios, para os projetos desportivos relacionados no anexo I.

Art. 3º Prorrogar o prazo de captação de recursos do projeto esportivo, para o qual o proponente fica autorizado a captar recurso, mediante doações e patrocínios, conforme anexo II.

Art. 4º Esta deliberação entra em vigor na data de sua publicação.

RICARDO CAPPELLI
Presidente da Comissão

ANEXO I

1 - Processo: 58701.002455/2011-11
Proponente: Paraná Esporte
Título: Jogos Escolares do Paraná 2012
Registro: 01PR087262011
Manifestação Desportiva: Desporto de Rendimento
CNPJ: 00.470.127/0001-74
Cidade: Curitiba - UF: PR
Valor aprovado para captação: R$ 2.806.787,04
Dados Bancários: Banco do Brasil Agência nº 3793 DV: 1 Conta Corrente (Bloqueada) Vinculada nº 9668-7
Período de Captação: da data de publicação até 30/03/2013.
2 - Processo: 58701.001647/2011-01
Proponente: Federação de Bodyboarding do Estado de São Paulo
Título: Circuito Paulista de Bodyboarding
Registro: 02SP081492011
Manifestação Desportiva: Desporto de Rendimento
CNPJ: 04.826.556/0001-92
Cidade: São Vicente - UF: SP
Valor aprovado para captação após recurso: R$ 311.355,03
Dados Bancários: Banco do Brasil Agência nº 0925 DV: 3 Conta Corrente (Bloqueada) Vinculada nº 40808-5
Período de Captação: da data de publicação até 15/07/2012.

ANEXO II

1 - Processo: 58000.005443/2008-32
Proponente: Federação Catarinense de Bocha e Bolão
Título: Plano Anual de Atividades Nacionais
Valor aprovado para captação: R$ 499.003,42
Dados Bancários: Banco do Brasil Agência nº 5203 DV: 5 Conta Corrente (Bloqueada) Vinculada nº 5274-4
Período de Captação: da data de publicação até 31/12/2012.

## DEPARTAMENTO DE GESTÃO INTERNA

### PORTARIA Nº 75, DE 5 DE JUNHO DE 2012

Dispõe sobre a descentralização externa de crédito orçamentário e repasse financeiro à UNIVERSIDADE FEDERAL DE SÃO PAULO/UNIFESP - Campus Baixada Santista e dá outras providências.

O DIRETOR DO DEPARTAMENTO DE GESTÃO INTERNA, no uso de suas atribuições, e tendo em vista a delegação de competência contida na Portaria ME nº 175, de 24 de setembro de 2008, resolve:

Art. 1º Autorizar a descentralização externa de créditos e o repasse de recursos financeiros para a UNIVERSIDADE FEDERAL DE SÃO PAULO/UNIFESP - Campus Baixada Santista, visando o apoio financeiro para "implantação de um Núcleo de Esporte de Alto Rendimento para Pessoas com Deficiência", conforme segue:

Órgão Cedente: Ministério do Esporte
Unidade Gestora: 180002 - Gestão: 00001 - Coordenação Geral de Planejamento, Orçamento e Finanças/Departamento de Gestão Interna.
Órgão Executor: UNIVERSIDADE FEDERAL DE SÃO PAULO/UNIFESP
Unidade Gestora: 153031 Gestão: 15250 ( Universidade Federal de São Paulo)
Programa: 2035
Ação: Preparação de Atletas.
Funcional Programática: 27.811.2035.20JN.0001
Natureza da despesa:
33.90.36 - R$ 14.400,00 (quatorze mil e quatrocentos reais)
Fonte: 100
44.90.52 - R$ 84.926,40 (oitenta e quatro mil, novecentos e vinte e seis reais e quarenta centavos)
Fonte: 118
Valor Projeto: R$ 99.326,40 (noventa e nove mil, trezentos e vinte seis reais e quarenta centavos)

Art. 2º Caberá à Secretária Nacional de Esporte de Alto Rendimento - SNEAR exercer o acompanhamento das ações previstas para execução do objeto dessa descentralização, de modo a evidenciar a boa e regular aplicação dos recursos transferidos.

Art. 3º A UNIVERSIDADE FEDERAL DE SÃO PAULO - UNIFESP deverá restituir ao Ministério do Esporte os créditos transferidos e não empenhados até o final do exercício de 2012.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

MÁRCIO SIMÃO

# Ministério do Meio Ambiente

## INSTITUTO BRASILEIRO DO MEIO AMBIENTE E DOS RECURSOS NATURAIS RENOVÁVEIS

### PORTARIA Nº 9, DE 5 DE JUNHO DE 2012

Institui a Política de Segurança da Informação, Informática e Comunicações (Posic) do Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (Ibama).

O PRESIDENTE DO INSTITUTO BRASILEIRO DO MEIO AMBIENTE E DOS RECURSOS NATURAIS RENOVÁVEIS - IBAMA, nomeado por Decreto de 16 de maio, publicado no Diário Oficial da União de 17 de maio de 2012, no uso das atribuições que lhe conferem o art.5º, parágrafo único do Decreto nº 6.099, de 26 de abril de 2007, que aprovou a Estrutura Regimental do IBAMA, publicado no Diário Oficial da União de 27 de abril de 2007 e art.5º do Regimento Interno aprovado pela Portaria nº GM/MMA nº 341 de 31 de agosto de 2011, publicada no Diário Oficial da União do dia subsequente, tendo em vista o disposto na Instrução Normativa nº 1 do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, e o que consta no Processo nº 02001.001654/2011-37; e

CONSIDERANDO a política que tem o objetivo de declarar o comprometimento da alta direção do Ibama com vistas a promover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a Gestão de Segurança da Informação e Comunicações neste Instituto;

CONSIDERANDO as diretrizes e princípios consignados na norma NBR ISO/IEC 27002 acerca do Código de Prática para a Gestão de Segurança da Informação;

CONSIDERANDO a Lei nº 8.159/1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados;

CONSIDERANDO o Decreto nº 1.171/1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

CONSIDERANDO a Lei nº 9.279/1996, que regula direitos e obrigações relativas à propriedade industrial;

CONSIDERANDO a Lei nº 9.609/1998, que dispõe acerca da proteção da propriedade intelectual de programa de computador e sua comercialização no Brasil;

CONSIDERANDO o Decreto nº 3.505/2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Lei nº 9.983/2000, que altera o Decreto-Lei nº 2.848/1940 (Código Penal), que dispõe sobre a tipificação de crimes por computador contra a Administração Pública;

CONSIDERANDO o Decreto nº 4.553/2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal;

CONSIDERANDO a Lei nº 10.650/2003, que dispõe sobre o acesso público aos dados e informações existentes nos órgãos e entidades integrantes do Sisnama;

CONSIDERANDO o Decreto nº 4.915/2003, que dispõe sobre o Sistema de Gestão de Documentos de Arquivo (Siga), da Administração Pública Federal;

CONSIDERANDO o Decreto nº 5.301/2004, que regulamenta o disposto na Medida Provisória nº 228, convertida na Lei nº 11.111/2005, que dispõe sobre a ressalva prevista na parte final do disposto no inciso XXXIII do art. 5º da Constituição Federal;

CONSIDERANDO a Lei nº 12.527/2011, que regula o acesso a informações previsto na Constituição Federal;

CONSIDERANDO a necessidade de assegurar a continuidade dos serviços, garantir a segurança dos sistemas, gerenciar a central de serviço e os incidentes, gerenciar a configuração, gerenciar mudanças, monitorar e avaliar o desempenho de TI e monitorar e avaliar os controles internos;

CONSIDERANDO a necessidade de viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação no âmbito do Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (Ibama), resolve:

Instituir a Política de Segurança da Informação, Informática e Comunicações (Posic) do Ibama.

Seção I - Dos Conceitos e Definições

Art. 1º Para fins da Política de Segurança da Informação, Informática e Comunicações considera-se:

I - Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;

II - Agente público: são todas as pessoas físicas que manifestam, por algum tipo de vínculo, a vontade do Estado, abarcando servidores, ocupantes de cargo comissionado ou em comissão, prestadores de serviço e estagiários;

III - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

IV - Análise de risco: uso sistemático de informações para identificar fontes e estimar o risco;

V - Avaliação de riscos: processo para comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

VI - Ativo: tudo que tenha ou gere valor para a organização;

VII - Ativos de informação: é o ativo composto por todos os dados, informações e conhecimentos gerados, armazenados e processados no Ibama, bem como os locais onde se encontram e as pessoas que têm acesso;

VIII - Classificação: grau de sigilo atribuído por autoridade competente a dados, informações, documentos, materiais, áreas ou instalações;

IX - Comitê de Segurança da Informação e Informática: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão ou entidade da Administração Pública Federal (APF);

X - Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais que podem ser de natureza administrativa, técnica, de gestão ou legal. Sinônimo para proteção ou contramedida;

XI - Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação, ou falta de controle, ou situação previamente desconhecida que possa ser relevante para a segurança da informação;

XII - Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e possíveis impactos nas operações de negociação, caso essas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes, reputação, marca da organização e suas atividades de valor agregado;

XIII - Gestão de riscos de segurança da informação e comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XIV - Gestão de segurança da informação e comunicações: ações e métodos que visam à integração das atividades de gestão de riscos e de continuidade de negociação, tratamento de incidentes e da informação, conformidade, credenciamento, segurança cibernética, física, lógica, orgânica e organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicação;

XV - Gestor de segurança da informação e informática: é o servidor público responsável pelas ações de segurança da informação e comunicações no Ibama;

XVI - Identificação de riscos: processo para localizar, listar e caracterizar elementos do risco;

XVII - Impacto: mudança adversa no nível obtido dos objetivos de negociações;

XVIII - Incidente: qualquer evento que não seja parte da operação-padrão do serviço e que cause ou possa causar interrupção ou redução na qualidade desse serviço;

XIX - Incidente de segurança da informação: é indicado por um, apenas, ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

XX - Informação: ativo que, como qualquer outro, é importante para os negócios, tem valor para a organização e, consequentemente, necessita ser adequadamente protegida, podendo existir de forma impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, mostrada em filmes ou falada em conversas;

XXI - Plano de Prevenção de Riscos: instrumento evolutivo, que tem como propósito reduzir os riscos de problemas quanto a segurança da informação;

XXII - Política de Segurança da Informação, Informática e Comunicações (Posic): documento aprovado pelo Ibama com as diretrizes e critérios relativos à segurança da informação e comunicações;

XXIII - Prestador de serviços: empresa privada que presta serviços diversos para o Ibama por meio de contrato de terceirização;

XXIV - Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;

XXV - Recursos de processamento da informação: qualquer sistema de processamento da informação, serviço, infraestrutura ou as instalações físicas que os abriguem;

XXVI - Riscos de segurança da informação e comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo na organização;

XXVII - Segurança da informação e comunicações (definição clássica): ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXVIII - Segurança da informação e comunicações (definição moderna): é a proteção da informação de vários tipos de ameaças para garantir a continuidade de negociações, minimizar seu risco e maximizar o retorno sobre os investimentos e as oportunidades;

XXIX - Termo de responsabilidade: termo assinado pelo usuário concordando em adotar todas as medidas cabíveis para garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade da informações que tiver acesso, bem como em assumir responsabilidades decorrentes de tal acesso;

XXX - Tratamento (processamento) da informação: recepção, produção, validação, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação, publicidade e controle da informação, inclusive as sigilosas;

XXXI - Usuários: agentes públicos e cidadãos com interesse nos serviços e/ou nas informações prestados pelo Ibama.

Seção II - Dos Princípios

Art. 2º A segurança da informação busca reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação, os recursos de processamento da informação ou os equipamentos de uma organização.

Art. 3º Para efeitos de aplicação desta política, são considerados princípios da segurança da informação:

I - a disponibilidade: propriedade de que a informação esteja acessível e utilizável por uma pessoa física, sistema, órgão ou entidade;

II - a confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados ou credenciados;

III - a integridade: propriedade de que a informação não esteja modificada ou destruída de maneira não autorizada ou acidental;

IV - a autenticidade: propriedade de que a informação seja produzida, expedida, modificada ou destruída por pessoa física, sistema, órgão ou entidade;

V - a confiabilidade: requer que os meios, nos quais a informação trafega e é armazenada, sejam preparados para promover e garantir eficientemente a recuperação dessa informação caso haja insucesso de mudança ou evento inesperado, com observância dos demais princípios de segurança;

VI - a responsabilidade: propriedade de que todo ativo possua um responsável que garanta sua correta utilização, além de monitorá-lo de maneira que o uso indevido seja reportado e as ações cabíveis tomadas.

Seção III - Do Objeto

Art. 4º As diretrizes de segurança da informação estabelecidas nesta Posic aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo Ibama, e que devem ser seguidas pelos agentes públicos da instituição e por todos os usuários que tenham acesso às informações da Instituição, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Parágrafo único. Seja qual for a forma ou o meio pelo qual a informação seja apresentada ou compartilhada, será sempre protegida adequadamente, de acordo com esta política.

Art. 5º Esta política aplica-se ao ambiente de trabalho e aos recursos de Tecnologia da Informação e Comunicação (TIC), estabelecendo responsabilidades e obrigações a todos os agentes públicos do Ibama que tenham acesso às informações ou aos recursos de TIC desta entidade.

Art. 6º O controle de acesso físico às instalações do Ibama, de acesso aos sistemas corporativos e às informações armazenadas, bem como o controle de circulação de pessoas e veículos serão regidos por norma complementar a esta Posic.

Art. 7º Esta Posic será difundida a todos os agentes públicos e cidadãos com interesse nos serviços prestados pelo Ibama através de um processo permanente de conscientização em Segurança da Informação.

Seção IV - Das Diretrizes Gerais

Art. 8º No Ibama, somente é permitido aos usuários o uso de recursos de processamento da informação disponibilizados pela Autarquia, de forma a garantir que os requisitos de segurança sejam atendidos.

Parágrafo único. Os chefes e os responsáveis pelas unidades organizacionais do Ibama autorizarão os acessos aos recursos de processamento de informação, conforme normas complementares que serão estabelecidas.

Art. 09º Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se de informações de forma não autorizada.

Art. 10º O cumprimento da política de segurança será auditado pela Auditoria do Ibama com a assessoria do Comitê de Segurança da Informação e Informática (CSII).

Art. 11º Os recursos de processamento da informação disponibilizados aos usuários terão suporte de um Plano de Prevenção de Riscos a fim de evitar situações de risco à segurança da informação.

Art. 12º Quaisquer recursos de processamento da informação serão testados em ambiente de homologação antes de serem colocados em produção.

Art. 13º É dever do agente público do Ibama conhecer e cumprir esta Política de Segurança da Informação, Informática e Comunicações.

Parágrafo único. A Posic estará disponível a todos os usuários do Ibama.

Art. 14º É condição para acesso aos ativos de informação do Ibama a adesão formal aos termos desta Política.

Art. 15º O agente público do Ibama é responsável pela segurança dos ativos de informação e processos que estejam sob sua responsabilidade.

Art. 16º Os gestores responsáveis pelos processos inerentes à gestão da segurança da informação receberão capacitação especializada.

Art. 17º Os contratos firmados pelo Ibama conterão cláusulas que determinem a observância desta política e das normas dela derivada.

Art. 18º Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pelo Ibama serão utilizados estritamente para seu propósito.

Parágrafo único. É vedado, a qualquer agente público do Ibama ou cooperados, o uso dos recursos de TIC para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem desta entidade, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações.

Seção V - Da Propriedade da Informação

Art. 19º A propriedade da informação será regida pelas seguintes diretrizes:

I - toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada pelos agentes públicos do Ibama e cooperados, no exercício de suas atividades, é de propriedade desta entidade e será protegida segundo estas diretrizes e nas regulamentações em vigor, conforme a classificação das informações, sem prejuízo da autoria, conforme definido em lei;

II - quando da obtenção de informação de terceiros, o gestor da informação providenciará, junto ao concedente, a documentação formal atinente aos direitos de acesso, antes de seu uso, conforme norma complementar;

III - na cessão de bases de dados nominais custodiadas ou na informação de propriedade do Ibama a terceiros, o gestor da informação providenciará a documentação formal relativa à autorização de acesso às informações, conforme norma complementar;

IV - procedimentos apropriados para garantir a conformidade dos requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e o uso de produtos de softwares proprietários;

V - privacidade e a proteção de dados que estejam em conformidade com as exigências das legislações relevantes, regulamentações e cláusulas contratuais.

Seção VI - Da Classificação e Tratamento da Informação

Art. 20º A classificação e o tratamento da informação observarão os seguintes requisitos e critérios:

I - o valor, requisitos legais, sensibilidade e criticidade da informação para o Ibama;

II - conjunto apropriado de procedimentos para rotulação e tratamento da informação que será definido e implementado de acordo com o critério de classificação adotado pelo Ibama;

Art. 21º Toda informação criada, manuseada, armazenada, transportada ou descartada do Ibama será classificada toda quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita;

Art. 22º A classificação e tratamento de informação serão:

I - norteadas pela legislação específica que disponha sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal (APF);

V - implementados e mantidos, em conformidade com a legislação vigente, visando a estabelecer os controles de segurança necessários a cada informação custodiada ou de propriedade do Ibama, ao longo do seu ciclo de vida; e

III - realizados de acordo com norma complementar específica sobre a matéria.

Art. 23º As informações sob gestão do Ibama terão segurança de maneira a serem adequadamente protegidas quanto ao acesso e uso, sendo que para as consideradas de alta criticidade, serão necessárias medidas especiais de tratamento;

Seção VII - Gestão de Incidentes de Segurança da Informação e Rede

Art. 24º A gestão de incidentes de segurança da informação e rede seguirá os seguintes critérios e procedimentos :

I - os incidentes de segurança da informação serão relatados por meio dos canais apropriados da Instituição, o mais rápido possível;

II - os agentes públicos usuários de sistemas e serviços de informação serão instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade de segurança em sistemas ou serviços;

III - serão observados os procedimentos de segurança da informação e comunicações, cada um com seu responsável, para assegurar respostas rápidas, efetivas e ordenadas;

IV - serão observados os procedimentos de gestão de incidentes de rede, cada um com seu responsável, para assegurar respostas rápidas, efetivas e ordenadas;

Art. 25º Soluções de contorno aplicadas para minimizar a ocorrência de incidentes de segurança serão temporárias e imediatamente submetidas ao gestor de segurança da informação e informática com definição do prazo para que a solução definitiva do problema seja implementada;

Art. 26º As evidências dos incidentes de segurança serão coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento, instituídas pelo órgão competente, nos casos em que um processo contra uma pessoa ou organização, após um incidente de segurança da informação.

Art. 27º A gestão de incidentes de segurança da informação deverá ser regida por norma complementar específica sobre a matéria.

Seção VIII - Do Gerenciamento de Riscos

Art. 28º A identificação das necessidades do Ibama em relação aos requisitos de segurança da informação será estabelecida mediante uma abordagem sistemática de gestão de riscos de segurança da informação.

Art. 29º A abordagem de gestão de riscos estará alinhada ao processo de gestão de risco de todas as áreas do Ibama.

Art. 30º O processo de gerenciamento de riscos será contínuo, com revisões periódicas a serem definidas pelo gestor de segurança da informação e informática.

Art. 31º O gerenciamento de riscos contemplará a definição preliminar de contexto, a análise/avaliação, o plano de tratamento, a aceitação, a implementação do plano de tratamento, o monitoramento e a análise crítica, a melhoria do processo de gestão e a comunicação dos riscos.

Art. 32º O processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) estará alinhado à metodologia denominada PDCA (Plan-Do-Check-Act), conforme definido na Norma Complementar nº 02/DSIC/GSIPR, de 13 de outubro de 2008, de modo a fomentar sua melhoria contínua.

Art. 33º A gestão dos riscos terá como objetivo subsidiar a segurança da informação e a continuidade da negociação;

Art. 34º O processo de gestão de riscos possibilitará a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança;

Art. 35º A gestão dos riscos seguirá os procedimentos definidos na Norma Complementar 04/IN01/DSIC/GSIPR de 14 de agosto de 2009.

Seção IX - Da Gestão de Continuidade de Negócio

Art. 36º O Ibama estabelecerá, em instrumento próprio, a Gestão de Continuidade de Negócio em Segurança da Informação e Comunicações, visando reduzir interrupção causada por desastres ou falhas nos recursos de TIC do Ibama.

Art. 37º Os eventos que possam causar interrupções nos processos do Ibama serão identificados quanto à probabilidade e seu impacto, e as consequências para a segurança da informação.

Art. 38º As medidas de proteção serão planejadas e os custos na aplicação de controles serão balanceados de acordo com os danos potenciais de falhas de segurança.

Art. 39º Toda informação institucional será mantida em local que a salvaguarde adequadamente.

Art. 40º Os planos de recuperação ou manutenção das operações serão desenvolvidos e implementados para assegurar a disponibilidade da informação no nível e escala de tempo requerido, após a ocorrência de interrupções ou falhas dos processos críticos.

Art. 41º Será mantida uma estrutura básica de planos de continuidade de operações e serviços para assegurar consistência, para contemplar os requisitos de segurança da informação e identificar prioridades de testes e manutenção.

Art. 42º Os planos de continuidade de operações e serviços serão testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

Art. 43º As unidades operacionais apresentarão semestralmente ao CSII os planos de continuidade de operações e serviços, ou suas atualizações, acompanhadas da análise e avaliação de risco atualizada.

Art. 44º O processo de gestão de riscos com vistas a minimizar possíveis impactos associados aos ativos será definido em norma complementar específica sobre a matéria.

Seção X - Do Monitoramento, Auditoria e Conformidade

Art. 45º O monitoramento, auditoria e conformidade observarão o seguinte:

I - o uso dos recursos de TIC disponibilizados pelo Ibama é passível de monitoramento e auditoria e deve ser implementado e mantido, sempre que possível, mecanismos que permitam a sua rastreabilidade;

II - a entrada e a saída de ativos de informação do Ibama, inclusive publicação e disponibilização, serão registradas e autorizadas por autoridade competente mediante procedimento formal;

III - as auditorias internas em segurança da informação serão reguladas por norma complementar formalizada e aprovada pela Auditoria Interna do Ibama.

Seção X - Do Controle de Acesso e Uso de Senhas

Art. 46º O controle de acesso e uso de senhas observará o seguinte:

I - o agente público do Ibama e das cooperadas que utilizam os recursos de TIC terá uma conta específica de acesso, pessoal e intransferível, cuja concessão será regulamentada em norma complementar;

II - os privilégios de leitura, modificação ou eliminação das informações serão definidos pelo gestor de cada setor ou unidade organizacional;

III - a autorização, o acesso, o uso da informação e dos recursos de TIC serão controlados e limitados ao cumprimento das atribuições de cada agente público do Ibama ou das cooperadas, e qualquer outra forma de uso necessita de prévia autorização formal do gestor de cada setor ou unidade organizacional;

IV - sempre que houver mudanças nas atribuições de determinado agente público do Ibama ou das cooperadas, será de responsabilidade da chefia imediata solicitar a adequação imediata dos privilégios de acesso às informações e dos recursos de TIC;

V - existirá um procedimento formal de registro, suspensão e bloqueio de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços;

VI - no caso de desvinculação temporária ou definitiva do agente público, os privilégios de acesso serão suspensos ou cancelados;

VII - os usuários serão orientados, de forma regular e periódica, a seguir as boas práticas de segurança da informação na seleção e uso de senhas;

VIII - equipamentos não monitorados e sob responsabilidade de agentes públicos possuirão um termo de responsabilidade assinado pelo agente público, de forma a assegurar que o equipamento seja adequadamente protegido;

IX - os usuários serão orientados a adotar uma política de mesa limpa e tela limpa;

X - os usuários receberão acesso somente a serviços que tenham sido especificamente autorizados a usar;

XI - os métodos de autenticação de usuários nos sistemas garantirão autenticação segura, conforme norma complementar;

XII - nas conexões advindas de localizações e equipamentos específicos serão implementadas identificações automáticas entre equipamentos como um meio de autenticar as conexões;

XIII - o acesso aos sistemas operacionais serão realizados por meio de procedimento seguro de entrada no sistema (logon);

XIV - os sistemas de gerenciamento de senhas serão interativos e assegurarão que sejam usadas senhas de qualidade;

XV - programas utilitários que possuam a capacidade de sobrepor os controles dos sistemas e aplicações serão de uso restrito e controlado; e

XVI - os horários de conexão serão restringidos de forma a assegurar segurança adicional para aplicações de alto risco.

Seção XI - Do Acesso à Internet, Uso do E-mail e Outros Recursos

Art. 47º O acesso à internet, uso de e-mail e outros recursos obedecerão ao seguinte:

I - a internet será utilizada para fins de complemento às atividades do setor, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos;

II - os recursos de internet, e-mail ou qualquer outro existente, ou que venham a ser adotados, não serão utilizados para a realização de trabalhos de terceiros ou de atividades que não sejam de interesse da Instituição ou que por ela não tenha sido autorizado;

§ 1º A norma complementar que discipline o uso do recurso de acesso à internet, e-mail ou qualquer outro recurso deverá ser elaborada e apresentada formalmente ao CSII, que decidirá pela sua aprovação.

§ 2º As normas complementares deverão disciplinar o uso dos recursos e estar formalmente acompanhadas de um Termo de Justificativa, que contemple a necessidade da disponibilização do recurso e de uma Análise de Riscos que apresente uma análise/avaliação dos riscos associados à liberação do recurso no que se refere à segurança da informação.

Seção XII - Da Gestão de Ativos

Art. 48º A gestão de ativos deverá observar ao seguinte:

I - todos os ativos deverão ser claramente identificados e um inventário desses ativos deve ser estruturado e mantido atualizado;

II - todas as informações e ativos associados a recursos de processamento da informação serão controladas pela unidade que dispõe do recurso ou serviço;

III - a unidade designará uma pessoa ou uma equipe que será responsável por acompanhar a produção, o desenvolvimento, a manutenção, o uso e a segurança do ativo;

IV - a eliminação de informações observará a norma complementar de procedimentos internos e classificação, e a temporalidade prevista na legislação;

V - os recursos de TIC disponibilizados para criação, manuseio, armazenamento, transporte e descarte da informação no Ibama disporão de mecanismos que minimizem os riscos inerentes aos problemas de segurança, a fim de evitar ocorrências de incidentes, de forma acidental ou intencional, que afetem os princípios da integridade, da disponibilidade e da confidencialidade das informações;

VI - os recursos de TIC utilizados pelo Ibama serão previamente homologados pelo Comitê de Tecnologia da Informação (CTI), identificados e inventariados individualmente pelas áreas competentes, além de possuir documentação mínima e atualizada para o seu uso, e estar em conformidade com as normas complementares de segurança.

Seção XIII - Da Segurança Física dos Equipamentos

Art. 49º A segurança física dos equipamentos obedecerão ao seguintes:

I - todas as áreas que contenham informações e instalações de processamento da informação serão protegidas por barreiras de segurança, tais como paredes, portões de entrada com controle adequado ou balcões de recepção com recepcionistas, definindo um perímetro de segurança para proteger essas áreas;

II - as áreas seguras serão protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso;

III - instalações, escritórios e salas possuirão projeto de segurança física, aprovado por órgão especialista em segurança, que contemple saídas de emergência, extintores posicionados de maneira estratégica e revisões periódicas das instalações;

IV - áreas seguras controladas pelo Ibama possuirão procedimentos adequados de proteção, bem como diretrizes que orientem o trabalho no interior dessas áreas, conforme norma complementar a ser estabelecida;

V - os equipamentos que operem fora das dependências do Ibama estarão sujeitos à norma complementar que trate de operações externas, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências do Ibama;

VI - a norma complementar de operações e computação móvel disciplinará e detalhará os procedimentos que assegurem a efetiva proteção dos equipamentos e da segurança da informação.

Seção XIV - Dos Serviços Terceirizados

Art. 50º Os serviços terceirizados seguirão ao seguinte:

I - todos os controles de segurança, as definições de serviço e os níveis de entrega incluídos em contratos de serviços terceirizados serão monitorados de forma que sejam implementados, executados e mantidos pela empresa terceirizada, em conformidade com o exigido nesta Política e nas normas dela derivadas;

II - os serviços, relatórios e registros fornecidos por terceiros serão regularmente monitorados, analisados criticamente e auditados;

III - as mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, procedimentos e controles existentes serão gerenciadas levando-se em conta a criticidade dos sistemas, os processos envolvidos e a reanálise/reavaliação dos riscos.

Seção XV - Do Planejamento e Aceitação dos Sistemas

Art. 51º O planejamento e aceitação dos sistemas do Ibama seguirão ao seguinte:

I - a utilização dos recursos será monitorada e sincronizada;

II - serão feitas projeções para necessidades de capacidade futura, para garantir o desempenho requerido do sistema;

III - serão estabelecidos, em ato próprio, critérios de aceitação para novos sistemas, atualizações, correções e novas versões;

IV - serão efetuados testes apropriados dos sistemas durante seu desenvolvimento e antes da sua aceitação, com a emissão do Relatório de Testes e do Termo de Homologação devidamente assinado pelo responsável do ativo;

V - serão implantados controles de detecção, prevenção e recuperação para a proteção contra códigos maliciosos, conforme norma complementar a ser definida;

VI - a infraestrutura de rede será adequadamente gerenciada e controlada, de forma a protegê-la contra ameaças, reduzir as vulnerabilidades e manter a segurança de sistemas e aplicações que utilizam essas redes, incluindo a informação em trânsito, conforme norma complementar a ser definida;

VII - as interconexões de sistemas internos e externos de informação do Ibama serão implementadas em conformidade com norma complementar de comunicação entre sistemas, que definirá regras, padrões e procedimentos a serem adotados, sempre se pautando nos padrões de interoperabilidade do Governo Federal (e-Ping);

VIII - as informações envolvidas em transações on-line originadas no Ibama serão protegidas para prevenir transmissões incompletas, erros de roteamento, alteração, divulgação, duplicação ou reapresentação de mensagem não autorizada;

IX - a integridade das informações disponibilizadas nos sistemas do Ibama e publicamente acessíveis serão protegidas para prevenir modificações não autorizadas;

X - o uso dos recursos de processamento de informação serão monitorados e os resultados das atividades de monitoramento serão analisadas criticamente, de forma regular;

XI - os registros (logs) serão protegidos contra a falsificação e acesso não autorizado;

XII - todas as atividades dos administradores e operadores do sistema serão registradas;

XIII - os relógios de todos os sistemas de processamento da informação relevantes, dentro do Ibama ou do domínio de segurança, serão sincronizados de acordo com a hora oficial.

Art. 52º É obrigatória a produção e manutenção, por período de tempo previamente determinado, registros (logs) que possam ser usados como trilha de auditoria, contendo atividades dos usuários, exceções e outros eventos de segurança da informação para auxiliar em futuras investigações e monitoramento de controle de acesso;

Seção XVI - Do Uso, Aquisição, Desenvolvimento e Manutenção de Sistema de Informação

Art. 53º O uso, aquisição, desenvolvimento e manutenção de sistema de informação observarão ao seguinte:

I - qualquer software que, por necessidade do serviço daquele setor, necessitar ser instalado, deverá ser comunicado com antecedência à área de Tecnologia da Informação do Ibama;

II - fica permanentemente proibida a instalação de quaisquer softwares sem licença de uso;

III - a área de Tecnologia da Informação do Ibama fica autorizada a desinstalar todo e qualquer software sem licença de uso;

IV - novos sistemas de informação ou a melhoria dos sistemas existentes devem ser especificados com requisitos de controle de segurança e dentro das especificações de requisitos estabelecidos com a área-fim do Ibama;

V - os dados de entrada de aplicações serão validados de forma a garantir que são corretos e apropriados;

VI - em todas as aplicações, serão incorporadas checagens de validação com o objetivo de detectar qualquer corrupção de informações por erros ou por ações deliberadas;

VII - os dados de saída das aplicações serão validados para assegurar que o processamento das informações armazenadas esteja correto e apropriado às circunstâncias;

VIII - a instalação de software em sistemas operacionais será controlada de forma a garantir o controle sobre as aplicações instaladas;

IX - o acesso ao código-fonte de aplicativo deverá ser restrito e controlado, caso esse aplicativo não esteja registrado sob licenças públicas;

X - a implementação de mudanças será controlada por meio de gerenciamento formal de mudanças;

XI - O gerenciamento de mudança deverá incluir:

a) a manutenção de um registro dos níveis acordados de autorização;

b) a garantia de que as mudanças sejam submetidas por usuários autorizados;

c) a análise crítica dos procedimentos de controle e integridade para assegurar que as mudanças não os comprometam;

d) a identificação de todo software, informação, entidades em bancos de dados e hardware que precisam de emendas;

e) a obtenção de aprovação formal para propostas detalhadas antes da implementação;

f) a garantia da aceitação das mudanças por usuários autorizados, antes da implementação;

g) a garantia da atualização da documentação do sistema após conclusão de cada mudança e de que a documentação antiga seja arquivada;

h) a manutenção de um controle de versão de todas as atualizações de softwares;

i) a manutenção de uma trilha para auditoria de todas as mudanças solicitadas;

j) a garantia de que toda a documentação operacional e procedimentos dos usuários sejam alterados conforme necessário e que se mantenham apropriados;

k) a garantia de que as mudanças sejam implementadas em horários apropriados, sem a perturbação dos processos de negócios cabíveis.

XII - o gerenciamento de mudanças será baseado no gerenciamento de configuração dos ativos do Ibama e pautado pela separação clara entre o ambiente de produção e o ambiente de teste.

XIII - o gerenciamento de mudanças garantirá o retorno ao estado anterior quando ocorrer alguma falha no procedimento;

XIV - as aplicações críticas do Instituto serão analisadas criticamente e testadas quando sistemas operacionais forem alterados (novas versões ou instalação de patches), para garantir que não haverá impacto adverso nas operações do Ibama ou na segurança;

XV - as informações acerca das vulnerabilidades técnicas dos sistemas de informação em uso serão obtidas em tempo hábil, avaliada a exposição do Instituto a essas vulnerabilidades, e tomadas as medidas apropriadas para lidar com os riscos associados;

XVI - todo servidor e prestador de serviço será ser treinado adequadamente para as questões de segurança;

Art. 54º Cabe à área de Tecnologia da Informação do Ibama, por meio de servidores designados, a supervisão e o monitoramento do desenvolvimento terceirizado de software de forma a garantir que critérios de segurança, qualidade, conformidade e desempenho sejam devidamente implementados;

Art. 55º As regras específicas de operação e manutenção em sistemas considerados críticos no Ibama serão definidas em norma complementar.

Art. 56º As regras específicas de operação e manutenção em soluções de Tecnologia da Informação e Comunicação serão definidas em norma complementar.

Seção XVII - Da Gestão de Controle, Rastreamento e Comunicação de Veículos, Embarcações e Aeronaves

Art. 57º A gestão de sistemas de controle, rastreamento e comunicação de veículos, embarcações e aeronaves do Ibama compreenderá a instituição de regras específicas de administração e utilização dos sistemas que envolvam controle, rastreamento e comunicação de veículos, embarcações e aeronaves, e será definida em norma complementar.

Seção XVIII - Da Gestão de Segurança na Comunicação

Art. 58º A gestão de segurança na comunicação seguirá às seguintes diretrizes:

I - a divulgação de informações nos meios de comunicação social, incluindo internet, estará de acordo com a política de comunicação do Ibama;

II - as informações e símbolos institucionais do órgão somente devem ser divulgadas com autorização do Presidente do Ibama ou gestor por ele delegado;

III - os servidores da Instituição não devem divulgar nos perfis pessoais de redes sociais imagens de servidores portando armas ou qualquer objeto ou símbolo de identificação do Ibama, sem prévia autorização;

IV - o servidor que vazar ou repassar, sem autorização, informações estratégicas, operacionais, de segurança e de inteligência do Órgão estará sujeito às sanções administrativas, cíveis e penais cabíveis.

Art. 59º As regras específicas da segurança na comunicação do Ibama serão estabelecidas em norma complementar;

Seção XIX - Da Gestão de Recursos Humanos

Art. 60º A gestão de Recursos Humanos observará ao seguintes:

II - os acessos dos servidores públicos aos sistemas corporativos ou aos sistemas disponibilizados ao Ibama deverão ser regulamentados, conforme norma complementar.

III - os prestadores de serviço do Ibama deverão conhecer e cumprir a Política de Segurança da Informação, Informática e Comunicações (Posic).

Art. 61º As regras específicas da segurança de gestão de recursos humanos do Ibama serão definidas em norma complementar;

Seção XX - Das Competências e Responsabilidades

Art. 62º A estrutura de Gestão de Segurança da Informação no Ibama será composta pelo Gestor de Segurança da Informação e Informática (GSII) e pelo Comitê de Segurança da Informação e Informática (CSII).

Art. 63º O Comitê de Segurança da Informação e Informática (CSII) terá a seguinte composição:

I - O Gestor de Segurança da Informação e Informática (GSII), que deverá ser designado pelo Presidente do Ibama.

II - Dois integrantes da Diretoria de Qualidade Ambiental (Diqua), designados pelo titular dessa diretoria;

III - Dois integrantes da Diretoria de Proteção Ambiental (Dipro), designados pelo titular dessa diretoria;

IV - Dois integrantes da Diretoria de Uso Sustentável da Biodiversidade e Floresta (Dbflo), designados pelo titular dessa diretoria;

V - Dois integrantes da Diretoria de Licenciamento Ambiental (Dilic), designados pelo titular dessa diretoria;

VI - Um integrante da Assessoria de Comunicação da Presidência do Ibama/Ascom, designado pela Presidência;

VII - Um integrante da Auditoria Interna (Audit), designado pelo titular da Auditoria Interna;

VIII - Dois integrantes da Área de TI do Ibama, designados pelo titular da Diretoria de Planejamento, Administração e Logística do Ibama;

IX - Um integrante da Área de Informações do Ibama/Cnia, designado pelo titular da Diretoria de Planejamento, Administração e Logística do Ibama/Diplan.

X - Um integrante da Área de Recursos Humanos, designado pelo titular da Coordenação-Geral de Recursos Humanos (Cgreh/Diplan).

Art. 64º O CSII deverá realizar reuniões periódicas para acompanhamento das atividades de segurança institucional, avaliação do cumprimento de metas de segurança e a efetiva aplicação dessa política.

Art. 65º O CSII realizará reuniões extraordinárias quando convocados pelo Gestor de Segurança de Informação e Informática.

Art. 66º O CSII deverá formar subgrupos, entre os seus integrantes, para realizar as seguintes atividades:

I - manter contato permanente com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, sob supervisão do GSII;

II - realizar vistorias em áreas e instalações, e produzir relatórios quanto à adequação dessas áreas aos requisitos de segurança, apresentando os resultados ao GSII;

III - realizar outras atividades relacionadas às suas atribuições.

Art. 67º São competências do Ibama, por meio do seu representante legal, no âmbito da Posic:

I - coordenar as ações de segurança da informação e comunicações;

II - aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança, por meio da Corregedoria da Instituição;

III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;

IV - nomear gestor de segurança da informação e informática;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VI - instituir Comitê de Segurança da Informação e Informática (CSII);

VII - remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Art. 68º São competências do Comitê de Segurança da Informação e Informática (CSII):

I - aprovar e revisar as diretrizes da Posic e suas regulamentações, que visam preservar a disponibilidade, a integridade e a confidencialidade das informações do Ibama;

II - assessorar na implementação das ações de segurança da informação e comunicações;

III - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

IV - avaliar e dar parecer acerca dos planos de continuidade de operações e serviços, ou as atualizações, apresentados semestralmente pelas unidades operacionais do Ibama;

V - propor alterações na Política de Segurança da Informação, Informática e Comunicações (Posic); VI - propor normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema;

VII - revisar, sempre que necessário, a Posic e todos os atos normativos dela decorrentes, não excedendo o período máximo de 3 anos.

§ 1º As revisões da Posic deverão ser precedidas da avaliação formal dos eventos e incidentes de segurança ocorridos no período anterior à revisão.

Art. 69º São competências do Gestor de Segurança da Informação e Informática:

I - presidir o Comitê de Segurança da Informação e Informática (CSII);

II - promover cultura de segurança da informação e comunicações;

III - promover a melhoria contínua dos processos de gestão de segurança da informação;

IV - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

V - propor recursos necessários às ações de segurança da informação e comunicações;

VI - coordenar o Comitê de Segurança da Informação e Informática e a equipe de tratamento e resposta a incidentes em redes computacionais;

VII - promover e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicações;

VIII - manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, para o trato de assuntos relativos à segurança da informação e comunicações;

IX - coordenar a gestão de riscos em segurança da informação realizada no Ibama;

X - propor normas relativas à segurança da informação e comunicações;

XI - propor e receber propostas de ajustes corretivos e de melhoria a serem incluídos nas revisões da Política de Segurança da Informação, Informática e Comunicações do Ibama (POSIC).

Art. 70º São responsabilidades atribuídas aos usuários que utilizam os recursos de processamento pertencentes ou controlados pelo Ibama:

I - conhecer e cumprir a Política de Segurança da Informação, Informática e Comunicações;

II - dentro das instalações do Ibama, portar crachá de identificação de maneira visível e/ou uniforme para os cargos que o exigirem;

III - manter sigilo e trocar periodicamente a senha pessoal;

IV - zelar pelas informações e equipamentos disponibilizados para a execução do seu serviço;

V - ao tomar conhecimento de qualquer incidente de segurança da informação, notificar o fato, imediatamente, ao CSII;

VI - participar de eventos promovidos pelo CSII relacionados à segurança de informação;

Art. 71º O cidadão, como principal cliente da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal direta e indireta, poderá apresentar sugestões de melhorias ou denúncias de quebra de segurança que deverão ser averiguadas pelas autoridades.

Seção XXI - Das Penalidades

Art. 72º A não observância dos preceitos desta política implicará na aplicação de sanções administrativas, cíveis e penais previstas no Estatuto do Servidor Público Federal (Lei n° 8.112/1990), no Código Penal (Decreto-Lei n° 2.848/1940, com as alterações da Lei n° 9.983/2000 e do Decreto n° 2.910/1998), no Código Civil (Lei nº 10.406/2002) ou na legislação que regule ou venha regular a matéria.

Seção XXII -Das Disposições Finais

Art. 73º Os agentes públicos do Ibama devem reportar à área de Tecnologia da Informação os incidentes em redes computacionais, conforme Norma Complementar nº 5 da IN nº 1 do Gabinete de Segurança Institucional (GSI) da Presidência da República.

Art. 74º Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação e Informática.

Art. 75º Revoga-se a Portaria IBAMA nº 23/2007.

Art. 76º Esta portaria entra em vigor na data de sua publicação.

VOLNEY ZANARDI JÚNIOR

# Ministério do Planejamento, Orçamento e Gestão

## SECRETARIA DO PATRIMÔNIO DA UNIÃO

### DESPACHOS

Declaro dispensada a licitação para a cessão em condições especiais ao Município de Maringá, de imóvel de propriedade da União com área de 14.471,34m² do pavilhão do armazém (com ônus), e o uso da área remanescente da cessão com 24.061,27 m² (sem ônus), localizado na data nº 08, quadra A-5, zona Armazém, no Município de Maringá, Estado do Paraná, com fulcro no art. 17, § 2º, inciso I, da Lei nº 8.666, de 21 de junho de 1993, com a redação dada pela Lei nº 11.196, de 21 de novembro de 2005, Processo nº 04936.002969/2008-81.

Curitiba, 29 de maio de 2012.
LUCIANO SABATKE DIZ
Superintendente do Patrimônio da União no Estado no Paraná
Substituto

No uso da competência que me foi atribuída pelo art. 32, inciso VI do anexo XII da Portaria MP nº 232, de 03 de agosto de 2005, RATIFICO a decisão do Superintendente Substituto do Patrimônio da União no Estado do Paraná, referente à dispensa de licitação (DOC CPROD 04936.002538/2012-09) para a cessão ao Município de Maringá, de imóvel de propriedade da União com área de 14.471,34m² do pavilhão do armazém (com ônus), e o uso da área remanescente da cessão com 24.061,27m² (sem ônus), localizado na data nº 08, quadra A-5, zona Armazém, no Município de Maringá, Estado do Paraná, de acordo com o que consta do processo nº 04936.002969/2008-81 e determino que seja publicada no Diário Oficial da União, no prazo de 05 (cinco) dias, conforme dispõe o art. 26 da Lei nº 8.666, de 21 de junho de 1993, com a redação dada pela Lei nº 11.107, de 06 de abril de 2005, Processo nº 04936.002969/2008-81.

Brasília, 1º de junho de 2012.
PAULA MARIA MOTTA LARA
Secretária do Patrimônio da União

## SUPERINTENDÊNCIA EM MINAS GERAIS

### PORTARIA Nº 33, DE 31 DE MAIO DE 2012

O SUPERINTENDENTE DO PATRIMÔNIO DA UNIÃO EM MINAS GERAIS, no uso de suas atribuições, em conformidade com o art. 40, inciso III, Anexo I do Decreto nº 7.063, de 13 de janeiro de 2010, o art. 32, inciso III, Anexo XII da Portaria MP nº 232, de 3 de agosto de 2005, Regimento Interno da Secretaria do Patrimônio da União, tendo em vista delegação de competência conferida pela Portaria SPU Nº 200, de 29 de junho de 2010, publicada no Diário Oficial da União nº 168, de 2/9/2009, Seção 2, página 46, nos termos dos arts. 538 a 553 do Código Civil Brasileiro, e dos elementos que integram o Processo nº 04926.000804/2011-99, resolve:

Art. 1º Aceitar a doação, com encargo, que faz o Município de Montes Claros/MG, com base na Lei Municipal nº 4.278, de 23 de novembro de 2010, para a União, de imóvel constituído por terreno com área de 2.865,00 m² (dois mil, oitocentos e sessenta e cinco metros quadrados), conforme descrição contida no art. 2º desta Portaria, situado no município de Montes Claros/MG, no Bairro Ibituruna, conforme matrícula n° 44.701, Livro nº 2-CU, "Registro Geral", às fls. 139, do 2º Ofício de Registro de Imóveis de Montes Claros.

Art. 2º O imóvel a ser doado possui as seguintes características e confrontações: "Um terreno com área de 2.865,00 m² (dois mil, oitocentos e sessenta e cinco metros quadrados), situado no bairro Ibituruna, nesta cidade de Montes Claros-MG, com os seguintes limites: partindo do alinhamento da Av. Norival Guilherme Vieira, com Av. Major Alexandre Rodrigues, segue pelo alinhamento da Av. Norival Guilherme Vieira na distancia de 50,00 metros, ponto inicial desta poligonal; dai, deflete a esquerda, formando um ângulo reto externo e segue na distancia de 79,78 metros; daí, deflete a direita, formando um ângulo reto interno e segue na distancia de 50,00 metros; daí, deflete à direita, novamente formando um ângulo reto interno e segue na distancia de 35,00 metros, até encontrar a Av. Major Alexandre Rodrigues; e daí, finalmente deflete a direita e segue pelo alinhamento da V. Major Alexandre Rodrigues, na distancia de 67,00 metros, até o ponto inicial desta poligonal".

Art. 3º O imóvel objeto desta Portaria destina-se à instalação e funcionamento da sede do Fórum da Justiça Especializada do Trabalho em Montes Claros e do Tribunal Regional do Trabalho da 3a Região.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

ROGÉRIO VEIGA ARANHA

### PORTARIA Nº 34, DE 31 DE MAIO DE 2012

O SUPERINTENDENTE DO PATRIMÔNIO DA UNIÃO EM MINAS GERAIS, no uso de suas atribuições, em conformidade com o art. 39, inciso III, Anexo I do Decreto nº 7.675, de 20 de janeiro de 2012, o art. 32, inciso III, Anexo XII da Portaria MP nº 232, de 3 de agosto de 2005, Regimento Interno da Secretaria do Patrimônio da União, tendo em vista delegação de competência conferida pela Portaria SPU Nº 200, de 29 de junho de 2010, publicada no Diário Oficial da União nº 168, de 2/9/2009, Seção 2, página 46, nos termos dos arts. 538 a 553 do Código Civil Brasileiro, e dos elementos que integram o Processo nº 04926.000780/2012-59, resolve:

Art. 1º Aceitar a doação, com encargo, que faz o Município de Sacramento, do imóvel constituído por área construída de 178,75 m² e respectivo terreno medindo 239,80 m², situado no município de Sacramento/MG, na Rua Silva Jardim, nº 04, conforme matrícula n° 013808, Livro Nº 2 - Registro Geral do Cartório de Registro de Imóveis de Sacramento/MG.

Art. 2º O imóvel a ser doado possui as seguintes características e confrontações: "IMÓVEL URBANO, situado nesta cidade de Sacramento, Estado de Minas Gerais, na RUA SILVA JARDIM nº 04, com a área construída de 178,75m2 e respectivo terreno medindo 239,80m2 (duzentos e trinta e nove metros quadrados e oitenta decímetros), contido dentro das seguintes divisas e confrontações: A FRENTE medindo 25,22 m (vinte e cinco metros e vinte e dois centímetros) confrontando com a faixa da Rua Silva Jardim; A LATERAL DIREITA, medindo 9,20m (nove metros e vinte centímetros) confrontando com imóvel pertencente a Daniel Afonso Rezende; A LATERAL ESQUERDA, 9,95m (nove metros e noventa e cinco centímetros) confrontando com a faixa da Avenida Visconde do Rio Branco, e finalmente AOS FUNDOS, partindo do alinhamento da Av. Visconde do Rio Branco, ou seja, da lateral esquerda, em direção a lateral direita do imóvel, segue numa extensão de 11,75m (onze metros e setenta e cinco centímetros), dai, defletindo a esquerda, fazendo ângulo interno, cuja abertura mede 175º 20´ , dai, segue numa extensão de 5,40m (cinco metros e quarenta centímetros), defletindo a direita, fazendo ângulo externo com a abertura de 173º 53´, dai segue numa extensão de 8,00m (oito metros), atingindo assim a lateral direita do imóvel, confrontando toda estas extensões, ou seja os fundos deste imóvel com a propriedade de Geraldo Magela de Carvalho e outros".

Art. 3º O imóvel objeto desta Portaria destina-se à instalação e funcionamento da sede do Tribunal Regional Eleitoral de Minas Gerais no município de Sacramento/MG.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

ROGÉRIO VEIGA ARANHA

### PORTARIA Nº 36, DE 5 DE JUNHO DE 2012

O SUPERINTENDENTE DO PATRIMÔNIO DA UNIÃO EM MINAS GERAIS, DA SECRETARIA DO PATRIMÔNIO DA UNIÃO, DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, no uso de suas atribuições, nos termos da Portaria SPU nº 6, de 31 de janeiro de 2001, do Art. 22 da Lei nº 9.636, de 15 de maio de 1998, do Art. 14 do Decreto nº 3.725, de 10/1/2001, e dos elementos que integram o Processo nº 04926.000935/2012-57, resolve:

Art. 1º Permitir o uso, a título ONEROSO e precário, no período de 6/6/2012 a 10/6/2012, ao Município de Pedro Leopoldo/MG, de área de 2.619,82m2, área essa que integra imóvel maior de propriedade da União (Matrícula nº 28.219, Livro 2, fls. 1-2, Registro Geral, Cartório de Registro de Imóveis de Pedro Leopoldo/MG, com 39,0536 hectares), situado em parte do local conhecido como Fazenda Modelo, Município de Pedro Leopoldo/MG.

Art. 2º A área a ser utilizada pelo Município de Pedro Leopoldo (2.619,82m2) possui a seguinte descrição: inicia-se no ponto 0149 definido pelas coordenadas N: 7.829.333,22 m e E: 600.481,15 m, deste segue com azimute de 231°05'56" e distância de 40,00m até o ponto V1 de coordenadas N: 7.829.308,10 m e E: 600.450,02 m, deste segue com azimute de 330°37'08" e distância de 76,00m até o ponto V2 de coordenadas N: 7.829.374,33 m e E: 600.412,73 m; deste segue com azimute de 80°01'00" e distância de 42,82m até o ponto D1 de coordenadas N: 7.829.381,75 m e E: 600.454,90 m,

Seção II - Dos Princípios

Art. 2º A segurança da informação busca reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação, os recursos de processamento da informação ou os equipamentos de uma organização.

Art. 3º Para efeitos de aplicação desta política, são considerados princípios da segurança da informação:

I - a disponibilidade: propriedade de que a informação esteja acessível e utilizável por uma pessoa física, sistema, órgão ou entidade;

II - a confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados ou credenciados;

III - a integridade: propriedade de que a informação não esteja modificada ou destruída de maneira não autorizada ou acidental;

IV - a autenticidade: propriedade de que a informação seja produzida, expedida, modificada ou destruída por pessoa física, sistema, órgão ou entidade;

V - a confiabilidade: requer que os meios, nos quais a informação trafega e é armazenada, sejam preparados para promover e garantir eficientemente a recuperação dessa informação caso haja insucesso de mudança ou evento inesperado, com observância dos demais princípios de segurança;

VI - a responsabilidade: propriedade de que todo ativo possua um responsável que garanta sua correta utilização, além de monitorá-lo de maneira que o uso indevido seja reportado e as ações cabíveis tomadas.

Seção III - Do Objeto

Art. 4º As diretrizes de segurança da informação estabelecidas nesta Posic aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo Ibama, e que devem ser seguidas pelos agentes públicos da instituição e por todos os usuários que tenham acesso às informações da Instituição, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Parágrafo único. Seja qual for a forma ou o meio pelo qual a informação seja apresentada ou compartilhada, será sempre protegida adequadamente, de acordo com esta política.

Art. 5º Esta política aplica-se ao ambiente de trabalho e aos recursos de Tecnologia da Informação e Comunicação (TIC), estabelecendo responsabilidades e obrigações a todos os agentes públicos do Ibama que tenham acesso às informações ou aos recursos de TIC desta entidade.

Art. 6º O controle de acesso físico às instalações do Ibama, de acesso aos sistemas corporativos e às informações armazenadas, bem como o controle de circulação de pessoas e veículos serão regidos por norma complementar a esta Posic.

Art. 7º Esta Posic será difundida a todos os agentes públicos e cidadãos com interesse nos serviços prestados pelo Ibama através de um processo permanente de conscientização em Segurança da Informação.

Seção IV - Das Diretrizes Gerais

Art. 8º No Ibama, somente é permitido aos usuários o uso de recursos de processamento da informação disponibilizados pela Autarquia, de forma a garantir que os requisitos de segurança sejam atendidos.

Parágrafo único. Os chefes e os responsáveis pelas unidades organizacionais do Ibama autorizarão os acessos aos recursos de processamento de informação, conforme normas complementares que serão estabelecidas.

Art. 09º Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se de informações de forma não autorizada.

Art. 10º O cumprimento da política de segurança será auditado pela Auditoria do Ibama com a assessoria do Comitê de Segurança da Informação e Informática (CSII).

Art. 11º Os recursos de processamento da informação disponibilizados aos usuários terão suporte de um Plano de Prevenção de Riscos a fim de evitar situações de risco à segurança da informação.

Art. 12º Quaisquer recursos de processamento da informação serão testados em ambiente de homologação antes de serem colocados em produção.

Art. 13º É dever do agente público do Ibama conhecer e cumprir esta Política de Segurança da Informação, Informática e Comunicações.

Parágrafo único. A Posic estará disponível a todos os usuários do Ibama.

Art. 14º É condição para acesso aos ativos de informação do Ibama a adesão formal aos termos desta Política.

Art. 15º O agente público do Ibama é responsável pela segurança dos ativos de informação e processos que estejam sob sua responsabilidade.

Art. 16º Os gestores responsáveis pelos processos inerentes à gestão da segurança da informação receberão capacitação especializada.

Art. 17º Os contratos firmados pelo Ibama conterão cláusulas que determinem a observância desta política e das normas dela derivada.

Art. 18º Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pelo Ibama serão utilizados estritamente para seu propósito.

Parágrafo único. É vedado, a qualquer agente público do Ibama ou cooperados, o uso dos recursos de TIC para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem desta entidade, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações.

Seção V - Da Propriedade da Informação

Art. 19º A propriedade da informação será regida pelas seguintes diretrizes:

I - toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada pelos agentes públicos do Ibama e cooperados, no exercício de suas atividades, é de propriedade desta entidade e será protegida segundo estas diretrizes e nas regulamentações em vigor, conforme a classificação das informações, sem prejuízo da autoria, conforme definido em lei;

II - quando da obtenção de informação de terceiros, o gestor da informação providenciará, junto ao concedente, a documentação formal atinente aos direitos de acesso, antes de seu uso, conforme norma complementar;

III - na cessão de bases de dados nominais custodiadas ou na informação de propriedade do Ibama a terceiros, o gestor da informação providenciará a documentação formal relativa à autorização de acesso às informações, conforme norma complementar;

IV - procedimentos apropriados para garantir a conformidade dos requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e o uso de produtos de softwares proprietários;

V - privacidade e a proteção de dados que estejam em conformidade com as exigências das legislações relevantes, regulamentações e cláusulas contratuais.

Seção VI - Da Classificação e Tratamento da Informação

Art. 20º A classificação e o tratamento da informação observarão os seguintes requisitos e critérios:

I - o valor, requisitos legais, sensibilidade e criticidade da informação para o Ibama;

II - conjunto apropriado de procedimentos para rotulação e tratamento da informação que será definido e implementado de acordo com o critério de classificação adotado pelo Ibama;

Art. 21º Toda informação criada, manuseada, armazenada, transportada ou descartada do Ibama será classificada toda quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita;

Art. 22º A classificação e tratamento de informação serão:

I - norteadas pela legislação específica que disponha sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal (APF);

V - implementados e mantidos, em conformidade com a legislação vigente, visando a estabelecer os controles de segurança necessários a cada informação custodiada ou de propriedade do Ibama, ao longo do seu ciclo de vida; e

III - realizados de acordo com norma complementar específica sobre a matéria.

Art. 23º As informações sob gestão do Ibama terão segurança de maneira a serem adequadamente protegidas quanto ao acesso e uso, sendo que para as consideradas de alta criticidade, serão necessárias medidas especiais de tratamento;

Seção VII - Gestão de Incidentes de Segurança da Informação e Rede

Art. 24º A gestão de incidentes de segurança da informação e rede seguirá os seguintes critérios e procedimentos :

I - os incidentes de segurança da informação serão relatados por meio dos canais apropriados da Instituição, o mais rápido possível;

II - os agentes públicos usuários de sistemas e serviços de informação serão instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade de segurança em sistemas ou serviços;

III - serão observados os procedimentos de segurança da informação e comunicações, cada um com seu responsável, para assegurar respostas rápidas, efetivas e ordenadas;

IV - serão observados os procedimentos de gestão de incidentes de rede, cada um com seu responsável, para assegurar respostas rápidas, efetivas e ordenadas;

Art. 25º Soluções de contorno aplicadas para minimizar a ocorrência de incidentes de segurança serão temporárias e imediatamente submetidas ao gestor de segurança da informação e informática com definição do prazo para que a solução definitiva do problema seja implementada;

Art. 26º As evidências dos incidentes de segurança serão coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento, instituídas pelo órgão competente, nos casos em que um processo contra uma pessoa ou organização, após um incidente de segurança da informação.

Art. 27º A gestão de incidentes de segurança da informação deverá ser regida por norma complementar específica sobre a matéria.

Seção VIII - Do Gerenciamento de Riscos

Art. 28º A identificação das necessidades do Ibama em relação aos requisitos de segurança da informação será estabelecida mediante uma abordagem sistemática de gestão de riscos de segurança da informação.

Art. 29º A abordagem de gestão de riscos estará alinhada ao processo de gestão de risco de todas as áreas do Ibama.

Art. 30º O processo de gerenciamento de riscos será contínuo, com revisões periódicas a serem definidas pelo gestor de segurança da informação e informática.

Art. 31º O gerenciamento de riscos contemplará a definição preliminar de contexto, a análise/avaliação, o plano de tratamento, a aceitação, a implementação do plano de tratamento, o monitoramento e a análise crítica, a melhoria do processo de gestão e a comunicação dos riscos.

Art. 32º O processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) estará alinhado à metodologia denominada PDCA (Plan-Do-Check-Act), conforme definido na Norma Complementar nº 02/DSIC/GSIPR, de 13 de outubro de 2008, de modo a fomentar sua melhoria contínua.

Art. 33º A gestão dos riscos terá como objetivo subsidiar a segurança da informação e a continuidade da negociação;

Art. 34º O processo de gestão de riscos possibilitará a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança;

Art. 35º A gestão dos riscos seguirá os procedimentos definidos na Norma Complementar 04/IN01/DSIC/GSIPR de 14 de agosto de 2009.

Seção IX - Da Gestão de Continuidade de Negócio

Art. 36º O Ibama estabelecerá, em instrumento próprio, a Gestão de Continuidade de Negócio em Segurança da Informação e Comunicações, visando reduzir interrupção causada por desastres ou falhas nos recursos de TIC do Ibama.

Art. 37º Os eventos que possam causar interrupções nos processos do Ibama serão identificados quanto à probabilidade e seu impacto, e as consequências para a segurança da informação.

Art. 38º As medidas de proteção serão planejadas e os custos na aplicação de controles serão balanceados de acordo com os danos potenciais de falhas de segurança.

Art. 39º Toda informação institucional será mantida em local que a salvaguarde adequadamente.

Art. 40º Os planos de recuperação ou manutenção das operações serão desenvolvidos e implementados para assegurar a disponibilidade da informação no nível e escala de tempo requerido, após a ocorrência de interrupções ou falhas dos processos críticos.

Art. 41º Será mantida uma estrutura básica de planos de continuidade de operações e serviços para assegurar consistência, para contemplar os requisitos de segurança da informação e identificar prioridades de testes e manutenção.

Art. 42º Os planos de continuidade de operações e serviços serão testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

Art. 43º As unidades operacionais apresentarão semestralmente ao CSII os planos de continuidade de operações e serviços, ou suas atualizações, acompanhadas da análise e avaliação de risco atualizada.

Art. 44º O processo de gestão de riscos com vistas a minimizar possíveis impactos associados aos ativos será definido em norma complementar específica sobre a matéria.

Seção X - Do Monitoramento, Auditoria e Conformidade

Art. 45º O monitoramento, auditoria e conformidade observarão o seguinte:

I - o uso dos recursos de TIC disponibilizados pelo Ibama é passível de monitoramento e auditoria e deve ser implementado e mantido, sempre que possível, mecanismos que permitam a sua rastreabilidade;

II - a entrada e a saída de ativos de informação do Ibama, inclusive publicação e disponibilização, serão registradas e autorizadas por autoridade competente mediante procedimento formal;

III - as auditorias internas em segurança da informação serão reguladas por norma complementar formalizada e aprovada pela Auditoria Interna do Ibama.

Seção X - Do Controle de Acesso e Uso de Senhas

Art. 46º O controle de acesso e uso de senhas observará o seguinte:

I - o agente público do Ibama e das cooperadas que utilizam os recursos de TIC terá uma conta específica de acesso, pessoal e intransferível, cuja concessão será regulamentada em norma complementar;

II - os privilégios de leitura, modificação ou eliminação das informações serão definidos pelo gestor de cada setor ou unidade organizacional;

III - a autorização, o acesso, o uso da informação e dos recursos de TIC serão controlados e limitados ao cumprimento das atribuições de cada agente público do Ibama ou das cooperadas, e qualquer outra forma de uso necessita de prévia autorização formal do gestor de cada setor ou unidade organizacional;

IV - sempre que houver mudanças nas atribuições de determinado agente público do Ibama ou das cooperadas, será de responsabilidade da chefia imediata solicitar a adequação imediata dos privilégios de acesso às informações e dos recursos de TIC;

V - existirá um procedimento formal de registro, suspensão e bloqueio de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços;

VI - no caso de desvinculação temporária ou definitiva do agente público, os privilégios de acesso serão suspensos ou cancelados;

VII - os usuários serão orientados, de forma regular e periódica, a seguir as boas práticas de segurança da informação na seleção e uso de senhas;

VIII - equipamentos não monitorados e sob responsabilidade de agentes públicos possuirão um termo de responsabilidade assinado pelo agente público, de forma a assegurar que o equipamento seja adequadamente protegido;

IX - os usuários serão orientados a adotar uma política de mesa limpa e tela limpa;

X - os usuários receberão acesso somente a serviços que tenham sido especificamente autorizados a usar;

XI - os métodos de autenticação de usuários nos sistemas garantirão autenticação segura, conforme norma complementar;

XII - nas conexões advindas de localizações e equipamentos específicos serão implementadas identificações automáticas entre equipamentos como um meio de autenticar as conexões;

XIII - o acesso aos sistemas operacionais serão realizados por meio de procedimento seguro de entrada no sistema (logon);

XIV - os sistemas de gerenciamento de senhas serão interativos e assegurarão que sejam usadas senhas de qualidade;

XV - programas utilitários que possuam a capacidade de sobrepor os controles dos sistemas e aplicações serão de uso restrito e controlado; e

XVI - os horários de conexão serão restringidos de forma a assegurar segurança adicional para aplicações de alto risco.

Seção XI - Do Acesso à Internet, Uso do E-mail e Outros Recursos

Art. 47º O acesso à internet, uso de e-mail e outros recursos obedecerão ao seguinte:

I - a internet será utilizada para fins de complemento às atividades do setor, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos;

II - os recursos de internet, e-mail ou qualquer outro existente, ou que venham a ser adotados, não serão utilizados para a realização de trabalhos de terceiros ou de atividades que não sejam de interesse da Instituição ou que por ela não tenha sido autorizado;

§ 1º A norma complementar que discipline o uso do recurso de acesso à internet, e-mail ou qualquer outro recurso deverá ser elaborada e apresentada formalmente ao CSII, que decidirá pela sua aprovação.

§ 2º As normas complementares deverão disciplinar o uso dos recursos e estar formalmente acompanhadas de um Termo de Justificativa, que contemple a necessidade da disponibilização do recurso e de uma Análise de Riscos que apresente uma análise/avaliação dos riscos associados à liberação do recurso no que se refere à segurança da informação.

Seção XII - Da Gestão de Ativos

Art. 48º A gestão de ativos deverá observar ao seguinte:

I - todos os ativos deverão ser claramente identificados e um inventário desses ativos deve ser estruturado e mantido atualizado;

II - todas as informações e ativos associados a recursos de processamento da informação serão controladas pela unidade que dispõe do recurso ou serviço;

III - a unidade designará uma pessoa ou uma equipe que será responsável por acompanhar a produção, o desenvolvimento, a manutenção, o uso e a segurança do ativo;

IV - a eliminação de informações observará a norma complementar de procedimentos internos e classificação, e a temporalidade prevista na legislação;

V - os recursos de TIC disponibilizados para criação, manuseio, armazenamento, transporte e descarte da informação no Ibama disporão de mecanismos que minimizem os riscos inerentes aos problemas de segurança, a fim de evitar ocorrências de incidentes, de forma acidental ou intencional, que afetem os princípios da integridade, da disponibilidade e da confidencialidade das informações;

VI - os recursos de TIC utilizados pelo Ibama serão previamente homologados pelo Comitê de Tecnologia da Informação (CTI), identificados e inventariados individualmente pelas áreas competentes, além de possuir documentação mínima e atualizada para o seu uso, e estar em conformidade com as normas complementares de segurança.

Seção XIII - Da Segurança Física dos Equipamentos

Art. 49º A segurança física dos equipamentos obedecerão ao seguintes:

I - todas as áreas que contenham informações e instalações de processamento da informação serão protegidas por barreiras de segurança, tais como paredes, portões de entrada com controle adequado ou balcões de recepção com recepcionistas, definindo um perímetro de segurança para proteger essas áreas;

II - as áreas seguras serão protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso;

III - instalações, escritórios e salas possuirão projeto de segurança física, aprovado por órgão especialista em segurança, que contemple saídas de emergência, extintores posicionados de maneira estratégica e revisões periódicas das instalações;

IV - áreas seguras controladas pelo Ibama possuirão procedimentos adequados de proteção, bem como diretrizes que orientem o trabalho no interior dessas áreas, conforme norma complementar a ser estabelecida;

V - os equipamentos que operem fora das dependências do Ibama estarão sujeitos à norma complementar que trate de operações externas, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências do Ibama;

VI - a norma complementar de operações e computação móvel disciplinará e detalhará os procedimentos que assegurem a efetiva proteção dos equipamentos e da segurança da informação.

Seção XIV - Dos Serviços Terceirizados

Art. 50º Os serviços terceirizados seguirão ao seguinte:

I - todos os controles de segurança, as definições de serviço e os níveis de entrega incluídos em contratos de serviços terceirizados serão monitorados de forma que sejam implementados, executados e mantidos pela empresa terceirizada, em conformidade com o exigido nesta Política e nas normas dela derivadas;

II - os serviços, relatórios e registros fornecidos por terceiros serão regularmente monitorados, analisados criticamente e auditados;

III - as mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, procedimentos e controles existentes serão gerenciadas levando-se em conta a criticidade dos sistemas, os processos envolvidos e a reanálise/reavaliação dos riscos.

Seção XV - Do Planejamento e Aceitação dos Sistemas

Art. 51º O planejamento e aceitação dos sistemas do Ibama seguirão ao seguinte:

I - a utilização dos recursos será monitorada e sincronizada;

II - serão feitas projeções para necessidades de capacidade futura, para garantir o desempenho requerido do sistema;

III - serão estabelecidos, em ato próprio, critérios de aceitação para novos sistemas, atualizações, correções e novas versões;

IV - serão efetuados testes apropriados dos sistemas durante seu desenvolvimento e antes da sua aceitação, com a emissão do Relatório de Testes e do Termo de Homologação devidamente assinado pelo responsável do ativo;

V - serão implantados controles de detecção, prevenção e recuperação para a proteção contra códigos maliciosos, conforme norma complementar a ser definida;

VI - a infraestrutura de rede será adequadamente gerenciada e controlada, de forma a protegê-la contra ameaças, reduzir as vulnerabilidades e manter a segurança de sistemas e aplicações que utilizam essas redes, incluindo a informação em trânsito, conforme norma complementar a ser definida;

VII - as interconexões de sistemas internos e externos de informação do Ibama serão implementadas em conformidade com norma complementar de comunicação entre sistemas, que definirá regras, padrões e procedimentos a serem adotados, sempre se pautando nos padrões de interoperabilidade do Governo Federal (e-Ping);

VIII - as informações envolvidas em transações on-line originadas no Ibama serão protegidas para prevenir transmissões incompletas, erros de roteamento, alteração, divulgação, duplicação ou reapresentação de mensagem não autorizada;

IX - a integridade das informações disponibilizadas nos sistemas do Ibama e publicamente acessíveis serão protegidas para prevenir modificações não autorizadas;

X - o uso dos recursos de processamento de informação serão monitorados e os resultados das atividades de monitoramento serão analisadas criticamente, de forma regular;

XI - os registros (logs) serão protegidos contra a falsificação e acesso não autorizado;

XII - todas as atividades dos administradores e operadores do sistema serão registradas;

XIII - os relógios de todos os sistemas de processamento da informação relevantes, dentro do Ibama ou do domínio de segurança, serão sincronizados de acordo com a hora oficial.

Art. 52º É obrigatória a produção e manutenção, por período de tempo previamente determinado, registros (logs) que possam ser usados como trilha de auditoria, contendo atividades dos usuários, exceções e outros eventos de segurança da informação para auxiliar em futuras investigações e monitoramento de controle de acesso;

Seção XVI - Do Uso, Aquisição, Desenvolvimento e Manutenção de Sistema de Informação

Art. 53º O uso, aquisição, desenvolvimento e manutenção de sistema de informação observarão ao seguinte:

I - qualquer software que, por necessidade do serviço daquele setor, necessitar ser instalado, deverá ser comunicado com antecedência à área de Tecnologia da Informação do Ibama;

II - fica permanentemente proibida a instalação de quaisquer softwares sem licença de uso;

III - a área de Tecnologia da Informação do Ibama fica autorizada a desinstalar todo e qualquer software sem licença de uso;

IV - novos sistemas de informação ou a melhoria dos sistemas existentes devem ser especificados com requisitos de controle de segurança e dentro das especificações de requisitos estabelecidos com a área-fim do Ibama;

V - os dados de entrada de aplicações serão validados de forma a garantir que são corretos e apropriados;

VI - em todas as aplicações, serão incorporadas checagens de validação com o objetivo de detectar qualquer corrupção de informações por erros ou por ações deliberadas;

VII - os dados de saída das aplicações serão validados para assegurar que o processamento das informações armazenadas esteja correto e apropriado às circunstâncias;

VIII - a instalação de software em sistemas operacionais será controlada de forma a garantir o controle sobre as aplicações instaladas;

IX - o acesso ao código-fonte de aplicativo deverá ser restrito e controlado, caso esse aplicativo não esteja registrado sob licenças públicas;

X - a implementação de mudanças será controlada por meio de gerenciamento formal de mudanças;

XI - O gerenciamento de mudança deverá incluir:

a) a manutenção de um registro dos níveis acordados de autorização;

b) a garantia de que as mudanças sejam submetidas por usuários autorizados;

c) a análise crítica dos procedimentos de controle e integridade para assegurar que as mudanças não os comprometam;

d) a identificação de todo software, informação, entidades em bancos de dados e hardware que precisam de emendas;

e) a obtenção de aprovação formal para propostas detalhadas antes da implementação;

f) a garantia da aceitação das mudanças por usuários autorizados, antes da implementação;

g) a garantia da atualização da documentação do sistema após conclusão de cada mudança e de que a documentação antiga seja arquivada;

h) a manutenção de um controle de versão de todas as atualizações de softwares;

i) a manutenção de uma trilha para auditoria de todas as mudanças solicitadas;

j) a garantia de que toda a documentação operacional e procedimentos dos usuários sejam alterados conforme necessário e que se mantenham apropriados;

k) a garantia de que as mudanças sejam implementadas em horários apropriados, sem a perturbação dos processos de negócios cabíveis.

XII - o gerenciamento de mudanças será baseado no gerenciamento de configuração dos ativos do Ibama e pautado pela separação clara entre o ambiente de produção e o ambiente de teste.

XIII - o gerenciamento de mudanças garantirá o retorno ao estado anterior quando ocorrer alguma falha no procedimento;

XIV - as aplicações críticas do Instituto serão analisadas criticamente e testadas quando sistemas operacionais forem alterados (novas versões ou instalação de patches), para garantir que não haverá impacto adverso nas operações do Ibama ou na segurança;

XV - as informações acerca das vulnerabilidades técnicas dos sistemas de informação em uso serão obtidas em tempo hábil, avaliada a exposição do Instituto a essas vulnerabilidades, e tomadas as medidas apropriadas para lidar com os riscos associados;

XVI - todo servidor e prestador de serviço será ser treinado adequadamente para as questões de segurança;

Art. 54º Cabe à área de Tecnologia da Informação do Ibama, por meio de servidores designados, a supervisão e o monitoramento do desenvolvimento terceirizado de software de forma a garantir que critérios de segurança, qualidade, conformidade e desempenho sejam devidamente implementados;

Art. 55º As regras específicas de operação e manutenção em sistemas considerados críticos no Ibama serão definidas em norma complementar.

Art. 56º As regras específicas de operação e manutenção em soluções de Tecnologia da Informação e Comunicação serão definidas em norma complementar.

Seção XVII - Da Gestão de Controle, Rastreamento e Comunicação de Veículos, Embarcações e Aeronaves

Art. 57º A gestão de sistemas de controle, rastreamento e comunicação de veículos, embarcações e aeronaves do Ibama compreenderá a instituição de regras específicas de administração e utilização dos sistemas que envolvam controle, rastreamento e comunicação de veículos, embarcações e aeronaves, e será definida em norma complementar.

Seção XVIII - Da Gestão de Segurança na Comunicação

Art. 58º A gestão de segurança na comunicação seguirá às seguintes diretrizes:

I - a divulgação de informações nos meios de comunicação social, incluindo internet, estará de acordo com a política de comunicação do Ibama;

II - as informações e símbolos institucionais do órgão somente devem ser divulgadas com autorização do Presidente do Ibama ou gestor por ele delegado;

III - os servidores da Instituição não devem divulgar nos perfis pessoais de redes sociais imagens de servidores portando armas ou qualquer objeto ou símbolo de identificação do Ibama, sem prévia autorização;

IV - o servidor que vazar ou repassar, sem autorização, informações estratégicas, operacionais, de segurança e de inteligência do Órgão estará sujeito às sanções administrativas, cíveis e penais cabíveis.

Art. 59º As regras específicas da segurança na comunicação do Ibama serão estabelecidas em norma complementar;

Seção XIX - Da Gestão de Recursos Humanos

Art. 60º A gestão de Recursos Humanos observará ao seguintes:

II - os acessos dos servidores públicos aos sistemas corporativos ou aos sistemas disponibilizados ao Ibama deverão ser regulamentados, conforme norma complementar.

III - os prestadores de serviço do Ibama deverão conhecer e cumprir a Política de Segurança da Informação, Informática e Comunicações (Posic).

Art. 61º As regras específicas da segurança de gestão de recursos humanos do Ibama serão definidas em norma complementar;

Seção XX - Das Competências e Responsabilidades

Art. 62º A estrutura de Gestão de Segurança da Informação no Ibama será composta pelo Gestor de Segurança da Informação e Informática (GSII) e pelo Comitê de Segurança da Informação e Informática (CSII).

Art. 63º O Comitê de Segurança da Informação e Informática (CSII) terá a seguinte composição:

I - O Gestor de Segurança da Informação e Informática (GSII), que deverá ser designado pelo Presidente do Ibama.

II - Dois integrantes da Diretoria de Qualidade Ambiental (Diqua), designados pelo titular dessa diretoria;

III - Dois integrantes da Diretoria de Proteção Ambiental (Dipro), designados pelo titular dessa diretoria;

IV - Dois integrantes da Diretoria de Uso Sustentável da Biodiversidade e Floresta (Dbflo), designados pelo titular dessa diretoria;

V - Dois integrantes da Diretoria de Licenciamento Ambiental (Dilic), designados pelo titular dessa diretoria;

VI - Um integrante da Assessoria de Comunicação da Presidência do Ibama/Ascom, designado pela Presidência;

VII - Um integrante da Auditoria Interna (Audit), designado pelo titular da Auditoria Interna;

VIII - Dois integrantes da Área de TI do Ibama, designados pelo titular da Diretoria de Planejamento, Administração e Logística do Ibama;

IX - Um integrante da Área de Informações do Ibama/Cnia, designado pelo titular da Diretoria de Planejamento, Administração e Logística do Ibama/Diplan.

X - Um integrante da Área de Recursos Humanos, designado pelo titular da Coordenação-Geral de Recursos Humanos (Cgreh/Diplan).

Art. 64º O CSII deverá realizar reuniões periódicas para acompanhamento das atividades de segurança institucional, avaliação do cumprimento de metas de segurança e a efetiva aplicação dessa política.

Art. 65º O CSII realizará reuniões extraordinárias quando convocados pelo Gestor de Segurança de Informação e Informática.

Art. 66º O CSII deverá formar subgrupos, entre os seus integrantes, para realizar as seguintes atividades:

I - manter contato permanente com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, sob supervisão do GSII;

II - realizar vistorias em áreas e instalações, e produzir relatórios quanto à adequação dessas áreas aos requisitos de segurança, apresentando os resultados ao GSII;

III - realizar outras atividades relacionadas às suas atribuições.

Art. 67º São competências do Ibama, por meio do seu representante legal, no âmbito da Posic:

I - coordenar as ações de segurança da informação e comunicações;

II - aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança, por meio da Corregedoria da Instituição;

III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;

IV - nomear gestor de segurança da informação e informática;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VI - instituir Comitê de Segurança da Informação e Informática (CSII);

VII - remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Art. 68º São competências do Comitê de Segurança da Informação e Informática (CSII):

I - aprovar e revisar as diretrizes da Posic e suas regulamentações, que visam preservar a disponibilidade, a integridade e a confidencialidade das informações do Ibama;

II - assessorar na implementação das ações de segurança da informação e comunicações;

III - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

IV - avaliar e dar parecer acerca dos planos de continuidade de operações e serviços, ou as atualizações, apresentados semestralmente pelas unidades operacionais do Ibama;

V - propor alterações na Política de Segurança da Informação, Informática e Comunicações (Posic); VI - propor normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema;

VII - revisar, sempre que necessário, a Posic e todos os atos normativos dela decorrentes, não excedendo o período máximo de 3 anos.

§ 1º As revisões da Posic deverão ser precedidas da avaliação formal dos eventos e incidentes de segurança ocorridos no período anterior à revisão.

Art. 69º São competências do Gestor de Segurança da Informação e Informática:

I - presidir o Comitê de Segurança da Informação e Informática (CSII);

II - promover cultura de segurança da informação e comunicações;

III - promover a melhoria contínua dos processos de gestão de segurança da informação;

IV - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

V - propor recursos necessários às ações de segurança da informação e comunicações;

VI - coordenar o Comitê de Segurança da Informação e Informática e a equipe de tratamento e resposta a incidentes em redes computacionais;

VII - promover e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicações;

VIII - manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, para o trato de assuntos relativos à segurança da informação e comunicações;

IX - coordenar a gestão de riscos em segurança da informação realizada no Ibama;

X - propor normas relativas à segurança da informação e comunicações;

XI - propor e receber propostas de ajustes corretivos e de melhoria a serem incluídos nas revisões da Política de Segurança da Informação, Informática e Comunicações do Ibama (POSIC).

Art. 70º São responsabilidades atribuídas aos usuários que utilizam os recursos de processamento pertencentes ou controlados pelo Ibama:

I - conhecer e cumprir a Política de Segurança da Informação, Informática e Comunicações;

II - dentro das instalações do Ibama, portar crachá de identificação de maneira visível e/ou uniforme para os cargos que o exigirem;

III - manter sigilo e trocar periodicamente a senha pessoal;

IV - zelar pelas informações e equipamentos disponibilizados para a execução do seu serviço;

V - ao tomar conhecimento de qualquer incidente de segurança da informação, notificar o fato, imediatamente, ao CSII;

VI - participar de eventos promovidos pelo CSII relacionados à segurança de informação;

Art. 71º O cidadão, como principal cliente da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal direta e indireta, poderá apresentar sugestões de melhorias ou denúncias de quebra de segurança que deverão ser averiguadas pelas autoridades.

Seção XXI - Das Penalidades

Art. 72º A não observância dos preceitos desta política implicará na aplicação de sanções administrativas, cíveis e penais previstas no Estatuto do Servidor Público Federal (Lei n° 8.112/1990), no Código Penal (Decreto-Lei n° 2.848/1940, com as alterações da Lei n° 9.983/2000 e do Decreto n° 2.910/1998), no Código Civil (Lei nº 10.406/2002) ou na legislação que regule ou venha regular a matéria.

Seção XXII -Das Disposições Finais

Art. 73º Os agentes públicos do Ibama devem reportar à área de Tecnologia da Informação os incidentes em redes computacionais, conforme Norma Complementar nº 5 da IN nº 1 do Gabinete de Segurança Institucional (GSI) da Presidência da República.

Art. 74º Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação e Informática.

Art. 75º Revoga-se a Portaria IBAMA nº 23/2007.

Art. 76º Esta portaria entra em vigor na data de sua publicação.

VOLNEY ZANARDI JÚNIOR

# Ministério do Planejamento, Orçamento e Gestão

## SECRETARIA DO PATRIMÔNIO DA UNIÃO

### DESPACHOS

Declaro dispensada a licitação para a cessão em condições especiais ao Município de Maringá, de imóvel de propriedade da União com área de 14.471,34m² do pavilhão do armazém (com ônus), e o uso da área remanescente da cessão com 24.061,27 m² (sem ônus), localizado na data nº 08, quadra A-5, zona Armazém, no Município de Maringá, Estado do Paraná, com fulcro no art. 17, § 2º, inciso I, da Lei nº 8.666, de 21 de junho de 1993, com a redação dada pela Lei nº 11.196, de 21 de novembro de 2005, Processo nº 04936.002969/2008-81.

Curitiba, 29 de maio de 2012.
LUCIANO SABATKE DIZ
Superintendente do Patrimônio da União no Estado no Paraná
Substituto

No uso da competência que me foi atribuída pelo art. 32, inciso VI do anexo XII da Portaria MP nº 232, de 03 de agosto de 2005, RATIFICO a decisão do Superintendente Substituto do Patrimônio da União no Estado do Paraná, referente à dispensa de licitação (DOC CPROD 04936.002538/2012-09) para a cessão ao Município de Maringá, de imóvel de propriedade da União com área de 14.471,34m² do pavilhão do armazém (com ônus), e o uso da área remanescente da cessão com 24.061,27m² (sem ônus), localizado na data nº 08, quadra A-5, zona Armazém, no Município de Maringá, Estado do Paraná, de acordo com o que consta do processo nº 04936.002969/2008-81 e determino que seja publicada no Diário Oficial da União, no prazo de 05 (cinco) dias, conforme dispõe o art. 26 da Lei nº 8.666, de 21 de junho de 1993, com a redação dada pela Lei nº 11.107, de 06 de abril de 2005, Processo nº 04936.002969/2008-81.

Brasília, 1º de junho de 2012.
PAULA MARIA MOTTA LARA
Secretária do Patrimônio da União

## SUPERINTENDÊNCIA EM MINAS GERAIS

### PORTARIA Nº 33, DE 31 DE MAIO DE 2012

O SUPERINTENDENTE DO PATRIMÔNIO DA UNIÃO EM MINAS GERAIS, no uso de suas atribuições, em conformidade com o art. 40, inciso III, Anexo I do Decreto nº 7.063, de 13 de janeiro de 2010, o art. 32, inciso III, Anexo XII da Portaria MP nº 232, de 3 de agosto de 2005, Regimento Interno da Secretaria do Patrimônio da União, tendo em vista delegação de competência conferida pela Portaria SPU Nº 200, de 29 de junho de 2010, publicada no Diário Oficial da União nº 168, de 2/9/2009, Seção 2, página 46, nos termos dos arts. 538 a 553 do Código Civil Brasileiro, e dos elementos que integram o Processo nº 04926.000804/2011-99, resolve:

Art. 1º Aceitar a doação, com encargo, que faz o Município de Montes Claros/MG, com base na Lei Municipal nº 4.278, de 23 de novembro de 2010, para a União, de imóvel constituído por terreno com área de 2.865,00 m² (dois mil, oitocentos e sessenta e cinco metros quadrados), conforme descrição contida no art. 2º desta Portaria, situado no município de Montes Claros/MG, no Bairro Ibituruna, conforme matrícula n° 44.701, Livro nº 2-CU, "Registro Geral", às fls. 139, do 2º Ofício de Registro de Imóveis de Montes Claros.

Art. 2º O imóvel a ser doado possui as seguintes características e confrontações: "Um terreno com área de 2.865,00 m² (dois mil, oitocentos e sessenta e cinco metros quadrados), situado no bairro Ibituruna, nesta cidade de Montes Claros-MG, com os seguintes limites: partindo do alinhamento da Av. Norival Guilherme Vieira, com Av. Major Alexandre Rodrigues, segue pelo alinhamento da Av. Norival Guilherme Vieira na distancia de 50,00 metros, ponto inicial desta poligonal; dai, deflete a esquerda, formando um ângulo reto externo e segue na distancia de 79,78 metros; daí, deflete a direita, formando um ângulo reto interno e segue na distancia de 50,00 metros; daí, deflete à direita, novamente formando um ângulo reto interno e segue na distancia de 35,00 metros, até encontrar a Av. Major Alexandre Rodrigues; e daí, finalmente deflete a direita e segue pelo alinhamento da V. Major Alexandre Rodrigues, na distancia de 67,00 metros, até o ponto inicial desta poligonal".

Art. 3º O imóvel objeto desta Portaria destina-se à instalação e funcionamento da sede do Fórum da Justiça Especializada do Trabalho em Montes Claros e do Tribunal Regional do Trabalho da 3a Região.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

ROGÉRIO VEIGA ARANHA

### PORTARIA Nº 34, DE 31 DE MAIO DE 2012

O SUPERINTENDENTE DO PATRIMÔNIO DA UNIÃO EM MINAS GERAIS, no uso de suas atribuições, em conformidade com o art. 39, inciso III, Anexo I do Decreto nº 7.675, de 20 de janeiro de 2012, o art. 32, inciso III, Anexo XII da Portaria MP nº 232, de 3 de agosto de 2005, Regimento Interno da Secretaria do Patrimônio da União, tendo em vista delegação de competência conferida pela Portaria SPU Nº 200, de 29 de junho de 2010, publicada no Diário Oficial da União nº 168, de 2/9/2009, Seção 2, página 46, nos termos dos arts. 538 a 553 do Código Civil Brasileiro, e dos elementos que integram o Processo nº 04926.000780/2012-59, resolve:

Art. 1º Aceitar a doação, com encargo, que faz o Município de Sacramento, do imóvel constituído por área construída de 178,75 m² e respectivo terreno medindo 239,80 m², situado no município de Sacramento/MG, na Rua Silva Jardim, nº 04, conforme matrícula n° 013808, Livro Nº 2 - Registro Geral do Cartório de Registro de Imóveis de Sacramento/MG.

Art. 2º O imóvel a ser doado possui as seguintes características e confrontações: "IMÓVEL URBANO, situado nesta cidade de Sacramento, Estado de Minas Gerais, na RUA SILVA JARDIM nº 04, com a área construída de 178,75m2 e respectivo terreno medindo 239,80m2 (duzentos e trinta e nove metros quadrados e oitenta decímetros), contido dentro das seguintes divisas e confrontações: A FRENTE medindo 25,22 m (vinte e cinco metros e vinte e dois centímetros) confrontando com a faixa da Rua Silva Jardim; A LATERAL DIREITA, medindo 9,20m (nove metros e vinte centímetros) confrontando com imóvel pertencente a Daniel Afonso Rezende; A LATERAL ESQUERDA, 9,95m (nove metros e noventa e cinco centímetros) confrontando com a faixa da Avenida Visconde do Rio Branco, e finalmente AOS FUNDOS, partindo do alinhamento da Av. Visconde do Rio Branco, ou seja, da lateral esquerda, em direção a lateral direita do imóvel, segue numa extensão de 11,75m (onze metros e setenta e cinco centímetros), dai, defletindo a esquerda, fazendo ângulo interno, cuja abertura mede 175º 20´ , dai, segue numa extensão de 5,40m (cinco metros e quarenta centímetros), defletindo a direita, fazendo ângulo externo com a abertura de 173º 53´, dai segue numa extensão de 8,00m (oito metros), atingindo assim a lateral direita do imóvel, confrontando toda estas extensões, ou seja os fundos deste imóvel com a propriedade de Geraldo Magela de Carvalho e outros".

Art. 3º O imóvel objeto desta Portaria destina-se à instalação e funcionamento da sede do Tribunal Regional Eleitoral de Minas Gerais no município de Sacramento/MG.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

ROGÉRIO VEIGA ARANHA

### PORTARIA Nº 36, DE 5 DE JUNHO DE 2012

O SUPERINTENDENTE DO PATRIMÔNIO DA UNIÃO EM MINAS GERAIS, DA SECRETARIA DO PATRIMÔNIO DA UNIÃO, DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, no uso de suas atribuições, nos termos da Portaria SPU nº 6, de 31 de janeiro de 2001, do Art. 22 da Lei nº 9.636, de 15 de maio de 1998, do Art. 14 do Decreto nº 3.725, de 10/1/2001, e dos elementos que integram o Processo nº 04926.000935/2012-57, resolve:

Art. 1º Permitir o uso, a título ONEROSO e precário, no período de 6/6/2012 a 10/6/2012, ao Município de Pedro Leopoldo/MG, de área de 2.619,82m2, área essa que integra imóvel maior de propriedade da União (Matrícula nº 28.219, Livro 2, fls. 1-2, Registro Geral, Cartório de Registro de Imóveis de Pedro Leopoldo/MG, com 39,0536 hectares), situado em parte do local conhecido como Fazenda Modelo, Município de Pedro Leopoldo/MG.

Art. 2º A área a ser utilizada pelo Município de Pedro Leopoldo (2.619,82m2) possui a seguinte descrição: inicia-se no ponto 0149 definido pelas coordenadas N: 7.829.333,22 m e E: 600.481,15 m, deste segue com azimute de 231°05'56" e distância de 40,00m até o ponto V1 de coordenadas N: 7.829.308,10 m e E: 600.450,02 m, deste segue com azimute de 330°37'08" e distância de 76,00m até o ponto V2 de coordenadas N: 7.829.374,33 m e E: 600.412,73 m; deste segue com azimute de 80°01'00" e distância de 42,82m até o ponto D1 de coordenadas N: 7.829.381,75 m e E: 600.454,90 m,