



**AGÊNCIA NACIONAL DE ÁGUAS
SUPERINTENDÊNCIA DE REGULAÇÃO**

RESOLUÇÕES DE 28 DE ABRIL DE 2014

O SUPERINTENDENTE DE REGULAÇÃO DA AGÊNCIA NACIONAL DE ÁGUAS - ANA, no exercício da competência a que se refere à Portaria nº 100, de 23 de maio de 2013, torna público que a DIRETORIA COLEGIADA, em sua 522ª Reunião Ordinária, realizada em 28 de abril de 2014, com fundamento no art. 12, inciso V, da Lei nº 9.984, de 17/07/2000, resolveu outorgar à:

Nº 661 - Ailton Nicoletti Babelo, Arroio Chuy, Município de Chuí/Rio Grande do Sul, irrigação.

Nº 662 - Heber Pena Jácome, rio Verde Grande, Município de Verdelândia/Minas Gerais, irrigação.

Nº 663 - Santa Colomba Agropecuária Ltda. - Faz. Caiçara Bom Nome, rio Itaguari, Município de Cocos/Bahia, irrigação.

Nº 664 - Santa Colomba Agropecuária Ltda. - Faz. Karitel, rio Itaguari, Município de Cocos/Bahia, irrigação.

Nº 665 - Santa Colomba Agropecuária Ltda. - Faz. Primavera, rio Itaguari, Município de Cocos/Bahia, irrigação.

O inteiro teor das Resoluções de outorga, bem como as demais informações pertinentes estarão disponíveis no site www.ana.gov.br.

O SUPERINTENDENTE DE REGULAÇÃO DA AGÊNCIA NACIONAL DE ÁGUAS - ANA, no exercício da competência a que se refere à Portaria nº 100, de 23 de maio de 2013, torna público que a DIRETORIA COLEGIADA, em sua 522ª Reunião Ordinária, realizada em 28 de abril de 2014, com fundamento no art. 12, inciso V, da Lei nº 9.984, de 17/07/2000, resolveu emitir as outorgas preventivas de uso de recursos hídricos à:

Nº 666 - Santa Colomba Agropecuária Ltda. - Faz. Portela, rio Itaguari, Município de Cocos/Bahia, irrigação.

Nº 667 - Santa Colomba Agropecuária Ltda. - Faz. Canguçu área 7, rio Itaguari, Município de Cocos/Bahia, irrigação.

Nº 668 - Santa Colomba Agropecuária Ltda. - Faz. Canguçu Área 06, rio Itaguari, Município de Cocos/Bahia, irrigação.

Nº 669 - Santa Colomba Agropecuária Ltda. - Faz. Rio do Meio Área 02, rio Itaguari, Município de Cocos/Bahia, irrigação.

Nº 670 - Santa Colomba Agropecuária Ltda. - Faz. Entre Rios 1015, rio Itaguari, Município de Cocos/Bahia, irrigação.

Nº 671 - Santa Colomba Agropecuária Ltda. - Faz. Garfo, rio Itaguari, Município de Cocos/Bahia, irrigação.

O inteiro teor das Resoluções, bem como as demais informações pertinentes estarão disponíveis no site www.ana.gov.br.

RODRIGO FLECHA FERREIRA ALVES

**INSTITUTO CHICO MENDES
DE CONSERVAÇÃO DA BIODIVERSIDADE**

PORTARIA Nº 52, DE 2 DE MAIO DE 2014

Modifica a composição do Conselho Consultivo da Estação Ecológica da Guanabara, no Estado do Rio de Janeiro.

O PRESIDENTE DO INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE - INSTITUTO CHICO MENDES, no uso das atribuições previstas pelo Decreto nº 7.515, de 08 de julho de 2011, e pela Portaria nº 304, de 28 de março de 2012, publicada no Diário Oficial da União de 29 de março de 2012;

Considerando o disposto no art. 29, da Lei nº 9.985, de 18 de julho de 2000, bem como, os arts. 17 a 20 do Decreto nº 4.340, de 22 de agosto de 2002, que a regulamentação;

Considerando o Plano Estratégico Nacional de Áreas Protegidas, instituído pelo Decreto nº 5.758/2006, que prevê como estratégias para aprimorar o planejamento e a gestão do SNUC o estabelecimento e a promoção do funcionamento dos conselhos das unidades de conservação, bem como o apoio à participação efetiva dos representantes das comunidades locais nos conselhos;

Considerando o Decreto S/Nº de 15 de fevereiro de 2006, que cria a Estação Ecológica da Guanabara;

Considerando a Instrução Normativa ICMBio nº 11, de 8 de junho de 2010, que disciplina as diretrizes, normas e procedimentos para a formação e funcionamento de Conselhos Consultivos em unidades de conservação federais;

Considerando a Portaria nº 42, de 29 de junho de 2011, publicada no Diário Oficial da União nº 124, de 30 de junho de 2011, seção 1, pág. 79 que cria o Conselho Consultivo da Estação Ecológica da Guanabara;

Considerando as proposições apresentadas pela Diretoria de Ações Socioambientais e Consolidação Territorial em Unidades de Conservação no Processo nº 02070.003598/2013-13, resolveu:

VIII- para acesso as informações e sistemas, todos os usuários devem ter identificador de uso pessoal, intransferível e com validade estabelecida, que permita de maneira clara o seu reconhecimento;

IX- o usuário deve ter acesso autorizado apenas às informações, instalações e recursos necessários e indispensáveis ao seu trabalho, de acordo com perfis definidos formalmente pelos gestores de TI e pelos requisitantes dos sistemas;

X- o usuário que tenha acesso a informações sigilosas somente poderá fazer uso deste para fins aprovados por seu superior imediato e pelo gestor das informações, quando houver gestor formalmente designado para aquele conjunto de dados, respeitando as regras de proteção estabelecidas;

XI- é dever do usuário manter-se a par dos procedimentos de segurança e do uso correto da informação e recursos computacionais de forma a minimizar possíveis riscos à segurança;

XII- para ter acesso às informações classificadas como sigilosas, o usuário deve firmar compromisso, em termo de sigilo e responsabilidade, quanto ao uso correto dos recursos e informações a que terá acesso autorizado;

XIII- quando do afastamento ou desligamento do usuário das suas atribuições faz-se necessário o cancelamento imediato dos direitos de acesso e uso da informação e dos acessos aos sistemas e preenchimento de termo de desligamento;

XIV- as credenciais de acesso (login e senha) e os recursos computacionais devem ser utilizados em conformidade com as normas específicas em vigor (Portaria MMA nº 197/2008 ou a que a suceder) e não podem ser utilizados para:

- a) constranger, assediar ou ameaçar qualquer pessoa;
- b) tentar, permitir ou causar alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicação;
- c) proporcionar benefícios financeiros próprios ou de terceiros;
- d) introduzir códigos maliciosos nos sistemas de informática;
- e) divulgar ou comercializar produtos, itens ou serviços;
- f) interferir, sem autorização, em um sistema, programa ou serviço; sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderindo ou cooperando com ataques, internos ou externos, de negação de serviços;

g) acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de informática, exceto quando autorizado pelo Gestor de Segurança da Informação, com o objetivo de realizar a gestão dos recursos de tratamento de incidentes;

h) monitorar ou interceptar o tráfego de informações nos sistemas de Tecnologia da Informação;

i) violar medidas de segurança ou de autenticação;

j) fornecer informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas, exceto mediante autorização de autoridade competente;

k) o armazenamento ou o uso de jogos em computador; e

l) o entretenimento durante o período de expediente.

XV- o Comitê de Segurança da Informação e Comunicações - CSIC deve criar, divulgar e manter planos de contingência e recuperação de desastres, formais e periodicamente testados, para garantir a continuidade das atividades críticas e o retorno à situação de normalidade, de acordo com os critérios e áreas responsáveis a serem definidos pelo CSIC;

XVI- todos os sistemas e equipamentos de informação, inclusive estações de trabalho, do MMA estão sujeitos a monitoração remota e eventual inspeção local, a fim de coibir a utilização indevida dos mesmos e danos resultantes desta utilização;

XVII- os incidentes de segurança, tais como: indícios de fraude, sabotagem ou falha na segurança em processos, sistemas, instalações ou equipamentos devem ser notificados imediatamente à chefia imediata e ao responsável pela gestão de segurança da informação e comunicações do MMA;

XVIII- todo o sistema em operação definido como crítico para os serviços prestados pelo MMA deve possuir documentação suficiente de forma a garantir sua manutenção, utilização, instalação, configuração, operação e produção, restringindo-se o acesso a essa documentação quando necessário; e

XIX- a entrada ou saída de equipamento computacional da instituição deve ser informada pelo detentor do equipamento, sendo o trânsito permitido somente mediante a autorização da autoridade competente.

Art. 8º Caso ocorra e/ou seja constatada a violação de uma ou mais das diretrizes constantes nesta Política de Segurança da Informação e Comunicações - POSIC, será aberta Sindicância e serão aplicadas as punições cabíveis.

Art. 9º O Subsecretário de Planejamento, Orçamento e Administração atua como Gestor de Segurança da Informação e Comunicações - GSIC, e possui as seguintes competências:

I- Promover cultura de segurança da informação e comunicações;

II- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III- Propor recursos necessários às ações de segurança da informação e comunicações;

IV- Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

V- Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI- 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;

VII- Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da Administração Pública Federal.

Art. 10. O Comitê de Segurança da Informação e Comunicações -CSIC será integrado por um representante de cada uma das seguintes unidades organizacionais da estrutura do MMA:

I- Gabinete da Secretaria Executiva - SECEX;
II- Consultoria Jurídica - CONJUR;
III- Assessor Especial de Controle Interno- AECI;
IV- Coordenação Geral de Tecnologia da Informação e Informática - CGTI ;

V- Assessoria de Comunicação Social - ASCOM; e
VI- Diretoria de Gestão Estratégica - DGE.

§ 1º Os representantes do CSIC, titulares e suplentes, serão designados por portaria do Secretário Executivo do MMA.

§ 2º Os membros do CSIC devem estar comprometidos com os seguintes procedimentos:

- a) apresentação de estudos, projetos e proposições relativas às competências do Comitê;
- b) proposição de alterações no Regimento Interno do CSIC quando necessário;
- c) proposição de prioridades em determinados assuntos;
- d) propor a implementação das decisões tomadas;
- e) indicação de representantes para participarem dos grupos de trabalho específicos do CSIC.

§ 3º Caberá ao GSIC convocar o gestor da unidade organizacional do MMA responsável pelo assunto em exame no Comitê para integrar os trabalhos do colegiado, bem como solicitar ao coordenador da área correspondente a indicação de assessor para participar dos trabalhos do Comitê, naquilo que afete àquela Coordenação.

Art. 11. Ao CSIC compete:

I- gerir a Política de Segurança da Informação e Comunicações do MMA;

II- coordenar as ações de Segurança da Informação e Comunicações do MMA;

III- estabelecer normas, padrões, procedimentos e demais aspectos necessários para assegurar a implementação da Política de Segurança da Informação e Comunicações do MMA;

IV- propor a regulamentação de matérias e alterações na Política de Segurança da Informação e Comunicações;

V- assessorar a Secretaria Executiva no aperfeiçoamento e na execução de ações de segurança da informação e comunicações do MMA;

VI- instituir grupos de trabalho ou subcomitês para tratar de temas e propor soluções específicas relacionados à segurança da informação e comunicações do MMA;

VII- comunicar à autoridade competente eventuais casos de quebra de segurança;

VIII- estabelecer e acompanhar o processo de auditoria de gestão da segurança da informação e comunicações;

IX- promover no MMA a cultura de segurança da informação e comunicações, elaborando e implementando, em articulação com a Coordenação Geral de Gestão de Pessoas, os programas destinados à conscientização e à capacitação dos recursos humanos que serão utilizados na consecução dos objetivos da Política da Segurança da Informação e Comunicações;

X- criar e avaliar os indicadores de acompanhamento da implantação dos planos estratégicos de segurança e tecnologia da informação e comunicações, bem como fiscalizar sua execução e propor medidas para correção; e

XI- elaborar e aprovar o seu regimento interno.

Art. 12. As reuniões do CSIC serão realizadas ordinariamente uma vez a cada três meses e, extraordinariamente, quando necessário.

§ 1º O aviso de convocação das reuniões, feito pelo Gestor de Segurança da Informação e Comunicações - GSIC, conterá a pauta de temas e de deliberações.

§ 2º Na reunião imediatamente subsequente, a ata deverá ser aprovada pelos membros do CSIC e assinada pelo Coordenador.

§ 3º Nas reuniões do CSIC, quando se tratar de assuntos sigilosos, deverá haver prévia indicação do grau de sigilo para adoção das medidas e dos procedimentos de segurança necessários.

§ 4º As deliberações do CSIC terão validade quando da reunião participarem, pelo menos, um terço dos integrantes do Comitê.

§ 5º As deliberações do CSIC serão tomadas por maioria simples dos votos dos representantes presentes.

§ 6º Durante suas ausências ou impedimentos excepcionais, os titulares serão substituídos por seus suplentes, cabendo a estes, nessa condição, o direito de votar nas reuniões.

§ 7º Havendo empate nas votações do CSIC, o Coordenador decidirá por voto de qualidade.

Art. 13. A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, deve permanecer operando no âmbito do MMA, observando-se o disposto na presente portaria.

Art. 14. Esta portaria entra em vigor na data de sua publicação.

IZABELLA TEIXEIRA