INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE

PORTARIA Nº 222, DE 23 DE agosto DE 2013.

Instituir a Política de Segurança da Informação e Comunicações - POSIC no âmbito do ICMBio.
(Processo nº 02070.000752/2013-03)

O PRESIDENTE DO INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE – INSTITUTO CHICO MENDES, no uso das competências atribuídas pelo artigo 21 do Decreto nº. 7.515, de 08 de julho de 2011 e pela Portaria nº. 304/Casa Civil, de 28 de março de 2012, publicada no Diário Oficial da União de 29 de março de 2012,

Considerando a Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

Considerando a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

Considerando a Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências;

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

Considerando o Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

Considerando a Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

Considerando a Norma Complementar nº 03/IN01/DSIC/GSIPR, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

Considerando a Norma Complementar nº 04/IN01/DSIC/GSICPR, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal;

Considerando a Norma Complementar nº 05/IN01/DSIC/GSICPR, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal;

Considerando a Norma Complementar nº 14/IN01/DSIC/GSICPR, que estabelece diretrizes relacionadas à segurança da informação e comunicações para uso de computação em nuvem nos órgãos e entidades da Administração Pública Federal;

Considerando a Normas ABNT NBR ISO/IEC 27001e 27002, que instituem o código de melhores práticas para gestão da segurança da informação,

RESOLVE:

CAPÍTULO I
DO ESCOPO

Art. 1º Instituir a Política de Segurança da Informação e Comunicações – POSIC que tem por escopo a instituição de diretrizes estratégicas visando assegurar a integridade de dados, informações e documentos do ICMBio, contra ameaças e vulnerabilidades, de modo a preservar os seus ativos, inclusive sua imagem institucional.

Art. 2º A POSIC trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do ICMBio, em todo o seu ciclo de duração - criação, manuseio, divulgação, armazenamento, transporte e descarte - visando a continuidade de seus processos vitais, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 3º Esta POSIC se aplica às unidades da estrutura regimental do ICMBio.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para efeitos desta POSIC fica estabelecido o significado dos seguintes termos e expressões:

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: aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao ICMBio;

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

IV - Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

V - Ativo: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha ou gere valor para a organização;

VI - Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VII - Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

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

IX - Comitê de Segurança da Informação e Comunicações: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do ICMBio;

X - Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

XI - 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;

XII - Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XIII - Credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

XIV - Criticidade: grau de importância da informação para a continuidade das atividades e serviços do ICMBio;

XV - Desastre: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

XVI - Descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XVII - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

XVIII - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

XIX - 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;

XX - 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;

XXI - 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;

XXII - 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;

XXIII - Gestor de segurança da informação e comunicações: é o servidor público responsável pelas ações de segurança da informação e comunicações no ICMBio;

XXIV - Incidente: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXV - Incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXVI - Informação: ativo que, como qualquer outro, é importante para os negócios, tem valor para a organização e, consequentemente, necessita ser adequadamente protegido, 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;

XXVII - Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVIII - Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação;

XXIX - Perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XXX - Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal, com o objetivo de fornecer diretrizes, critérios e

suporte administrativo suficientes à implementação da segurança da informação e comunicações;

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

XXXII - Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;

XXXIII - 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;

XXXIV - Segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, garantindo a continuidade de negociações, minimizando seu risco e maximizando o retorno sobre os investimentos e as oportunidades;

XXXV - Serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

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

XXXVII - Tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XXXVIII - Tempo Objetivo de Recuperação: é o tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente;

XXXIX - Usuário: agente público que obteve autorização do responsável pela área interessada para acesso aos ativos de Informação do ICMBio;

XL - Vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 5° 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 integridade: propriedade de que a informação não esteja modificada ou destruída de maneira não autorizada ou acidental;

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

IV - 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;

V - a publicidade: dar transparência no trato da informação, observados os critérios legais;

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;

VII - a ética: os direitos dos agentes públicos devem ser preservados, sem o comprometimento da Segurança da Informação e Comunicações.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 6º As diretrizes de segurança da informação estabelecidas nesta POSIC aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo ICMBio, e que devem ser seguidas pelos agentes públicos, 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. 7º Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pelo ICMBio serão utilizados estritamente para seu propósito.

Parágrafo único. É vedado a qualquer agente público do ICMBio o uso dos recursos de Tecnologia da Informação e Comunicações 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.

Da Seção I
Da Gestão da Segurança da Informação e Comunicações

Art. 8º A Gestão da Segurança da Informação e Comunicações não se limita à tecnologia da informação e comunicações, compreendendo as ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética,

segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos.

Art. 9º Toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas atividades no ICMBio, é considerada um bem e propriedade do Instituto e deve ser protegida segundo as diretrizes descritas nesta Política e demais regulamentações em vigor.

Seção II
Da Propriedade da Informação

Art. 10 A propriedade da informação será regida pelas seguintes diretrizes:

I - toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada por usuários que tenham acesso às informações do ICMBio, no exercício de suas atividades, é de propriedade desta entidade e será protegida segundo estas diretrizes e 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;

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

Seção III
Da Classificação e Tratamento da Informação

Art. 11 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 ICMBio;

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 ICMBio;

Art. 12 Toda informação criada, manuseada, armazenada, transportada ou descartada do ICMBio será classificada de acordo com a Lei nº 12.527, de 18 de novembro de 2011.

Art. 13 As informações sob gestão do ICMBio 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 com o objetivo de limitar a exploração às informações exclusivas do Instituto.

Seção IV
Do Tratamento de Incidentes de Rede

Art. 14 A área de tecnologia da informação manterá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, instituída pelo Comitê de Segurança da

Informação e Comunicações, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

Seção V
Da Gestão de Riscos

Art. 15 O Processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC - será implementado considerando, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do ICMBio e estará alinhado à metodologia denominada PDCA (Plan-Do-Check-Act), observando diretrizes e normas específicas no âmbito da Administração Pública Federal, de modo a fomentar sua melhoria contínua.

Seção VI
Da Gestão de Continuidade

Art. 16 As unidades descentralizadas do ICMBio devem manter processo de gestão de continuidade das atividades e serviços, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil, quando for o caso.

Art. 17 Aprovado pelo Comitê de Segurança da Informação e Comunicações, a área de tecnologia da informação do ICMBio deverá manter Plano de Contingências, gradado de acordo com o grau de probabilidade de ocorrência do evento ou sinistro, estabelecendo o conjunto de estratégias e procedimentos que devem ser adotados em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

Parágrafo único. As medidas constantes do Plano de Contingências devem minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

Seção VII
Do Monitoramento, Auditoria e Conformidade

Art. 18 O monitoramento, auditoria e conformidade observarão o seguinte:

I - o uso dos recursos de tecnologia da informação e comunicações disponibilizados pelo ICMBio é passível de monitoramento e auditoria e devem ser implementados e mantidos, sempre que possível, mecanismos que permitam a sua rastreabilidade;

II - a entrada e a saída de ativos de informação do ICMBio serão registradas e autorizadas por autoridade competente mediante procedimento formal;

III - A área de tecnologia da informação manterá registros e procedimentos, como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, à rede interna e à internet.

Seção VIII
Dos Controles de Acesso e Uso de Senhas

Art. 19 O controle de acesso e uso de senhas observará o seguinte:

I – o usuário que utiliza os recursos de TIC terá uma conta específica de acesso, pessoal e intransferível, conforme norma interna;

II - a autorização, o acesso, o uso da informação e dos recursos de tecnologia da informação e comunicações serão controlados e limitados ao cumprimento das atribuições de cada usuário, e qualquer outra forma de uso necessita de prévia autorização formal do gestor de cada setor ou unidade organizacional;

III - no caso de desvinculação temporária ou definitiva do usuário, os privilégios de acesso serão suspensos ou cancelados;

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

Seção IX
Do Uso de e-mail

Art. 20 O correio eletrônico é um meio de comunicação corporativa do ICMBio.

§ 1° As regras de acesso e utilização de e-mail institucional devem atender às orientações desta POSIC, norma interna e demais diretrizes do Governo.

§ 2° A área de tecnologia deverá manter os controles do uso e cancelamento de acesso ao correio eletrônico.

Seção X
Do Acesso à Internet

Art. 21 O acesso à rede mundial de computadores - internet, no ambiente de trabalho, deverá ser regido por norma interna, atendendo esta POSIC e demais orientações governamentais e legislação em vigor.

Seção XI
Da Computação em Nuvem

Art. 22 O ICMBio poderá utilizar de tecnologias de Computação em Nuvem, desde que em conformidade com as diretrizes e normas específicas relacionadas à Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal.

Parágrafo único. Ao Gestor de Segurança da Informação e Comunicações, no âmbito de suas atribuições, cabe propor ações de segurança da informação e comunicações para a implementação ou contratação, no ICMBio, de tecnologias de computação em nuvem.

Seção XII
Do Uso, Aquisição, Desenvolvimento e Manutenção de Sistema de Informação

Art. 23 O uso, aquisição, desenvolvimento e manutenção de sistema de informação observarão as seguintes regras:

I – fica proibida permanentemente a instalação de quaisquer softwares sem licença de uso;

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

III - 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 ICMBio;

IV - o gerenciamento de mudanças deve incluir a garantia de que suas implementações sejam realizadas em horários apropriados, sem a perturbação dos processos de negócios cabíveis.

Art. 24 Cabe à área de Tecnologia da Informação do ICMBio, 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.

CAPÍTULO V
DAS PENALIDADES

Art. 25 O agente público responderá administrativa, civil e/ou penalmente pelo prejuízo que vier a ocasionar ao ICMBio, em decorrência do descumprimento das regras previstas nesta POSIC e demais normas internas e legislação vigente.

CAPÍTULO VI
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 26 A estrutura de Gestão de Segurança da Informação e Comunicações no ICMBio será composta pelo Gestor de Segurança da Informação e Comunicações (GSIC) e pelo Comitê de Segurança da Informação e Comunicações (CSIC).

Art. 27 O CSIC 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. 28 O CSIC realizará reuniões extraordinárias quando convocados pelo Gestor de Segurança de Informação e Comunicações.

Art. 29 Compete à Presidência do ICMBio, no âmbito da POSIC:

I - Promover cultura de segurança da informação e comunicações;

II - instituir Comitê de Segurança da Informação e Comunicações (CSIC);

III - nomear Gestor de Segurança da Informação e Comunicações;

IV - aprovar a POSIC e demais normas de segurança da informação e comunicações;

V - instituir a Equipe de Tratamento e Resposta a incidentes em redes computacionais;

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

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);

VIII - aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança.

Art. 30 Compete ao Gestor de Segurança da Informação e Comunicações do ICMBio:

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 - coordenar as ações de segurança da informação e comunicações;

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

VII - 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;

VIII - Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do ICMBio;

IX - Providenciar a divulgação interna desta POSIC.

Art. 31 Compete ao Comitê de Segurança da Informação e Comunicações (CSIC), no âmbito da POSIC:

I - Promover cultura de segurança da informação e comunicações;

II - Assessorar na implementação das ações de segurança da informação e comunicações no ICMBio;

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

IV - Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

CAPÍTULO VII
DA ATUALIZAÇÃO

Art. 32 Esta portaria deverá ser revisada e atualizada, no máximo, a cada três anos, a contar da data de sua publicação.

Art. 33 As áreas têm prazo de noventa dias, a contar da publicação desta POSIC, para submeterem ao Comitê de Segurança da Informação e Comunicações - CSIC proposta de atualização ou criação das normas internas complementares e específicas sobre segurança da informação e comunicações.

Art. 34 Esta portaria entra em vigor na data de sua publicação.

ROBERTO RICARDO VIZENTIN
Presidente

PUBLICADA NO BS Nº 34
DE 23/08/2013.

PRESIDÊNCIA

PORTARIA

O PRESIDENTE DO INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE, no uso das competências atribuídas pelo artigo 21 do Decreto nº. 7.515, de 08 de julho de 2011, pela Portaria nº. 304/Casa Civil, de 28 de março de 2012, publicada no Diário Oficial da União de 29 de março de 2012, RESOLVE:

Nº401, de 23.08.2013 - Art. 1º Dispensar a servidora CAROLINA MATOSINHO ALVITE, matrícula SIAPE nº 1338269, do Grupo de Trabalho - GT instituído pela Portaria nº 119, de 22 de março de 2013, publicado no Boletim de Serviço nº 12, de 22 de março de 2013 e das atividades de relatoria do GT.

Art. 2º Designar o servidor MARCELO DERZI VIDAL, matrícula SIAPE nº 1443243, para compor o Grupo de Trabalho - GT instituído pela Portaria nº 119, de 22 de março de 2013, publicado no Boletim de Serviço nº 12, de 22 de março de 2013, bem como desempenhar a atividade de relatoria do GT.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

ROBERTO RICARDO VIZENTIN

PORTARIA NORMATIVA

Instituir a Política de Segurança da Informação e Comunicações - POSIC no âmbito do ICMBio.

(Processo nº 02070.000752/2013-03)

O PRESIDENTE DO INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE – INSTITUTO CHICO MENDES, no uso das competências atribuídas pelo artigo 21 do Decreto nº. 7.515, de 08 de julho de 2011 e pela Portaria nº. 304/Casa Civil, de 28 de março de 2012, publicada no Diário Oficial da União de 29 de março de 2012,

Considerando a Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

Considerando a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

Considerando a Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências;

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

Considerando o Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

Considerando a Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

Considerando a Norma Complementar nº 03/IN01/DSIC/GSIPR, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

Considerando a Norma Complementar nº 04/IN01/DSIC/GSICPR, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal;
Considerando a Norma Complementar nº 05/IN01/DSIC/GSICPR, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal;
Considerando a Norma Complementar nº 14/IN01/DSIC/GSICPR, que estabelece diretrizes relacionadas à segurança da informação e comunicações para uso de computação em nuvem nos órgãos e entidades da Administração Pública Federal;
Considerando a Normas ABNT NBR ISO/IEC 27001e 27002, que instituem o código de melhores práticas para gestão da segurança da informação, RESOLVE:

CAPÍTULO I
DO ESCOPO

Nº222, de 23.08.2013 - Art. 1º Instituir a Política de Segurança da Informação e Comunicações – POSIC que tem por escopo a instituição de diretrizes estratégicas visando assegurar a integridade de dados, informações e documentos do ICMBio, contra ameaças e vulnerabilidades, de modo a preservar os seus ativos, inclusive sua imagem institucional.
Art. 2º A POSIC trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do ICMBio, em todo o seu ciclo de duração - criação, manuseio, divulgação, armazenamento, transporte e descarte - visando a continuidade de seus processos vitais, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.
Art. 3º Esta POSIC se aplica às unidades da estrutura regimental do ICMBio.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para efeitos desta POSIC fica estabelecido o significado dos seguintes termos e expressões:
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: aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao ICMBio;
III - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
IV - Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;
V - Ativo: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha ou gere valor para a organização;
VI - Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VII - Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
VIII - Classificação: grau de sigilo atribuído por autoridade competente, a dados, informações, documentos, materiais, áreas ou instalações;
IX - Comitê de Segurança da Informação e Comunicações: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do ICMBio;
X - Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
XI - 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;
XII - Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
XIII - Credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;
XIV - Criticidade: grau de importância da informação para a continuidade das atividades e serviços do ICMBio;
XV - Desastre: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;
XVI - Descarte: eliminação correta de informações, documentos, mídias e acervos digitais;
XVII - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
XVIII - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;
XIX - 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;
XX - 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;
XXI - 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;

XXII - 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;
XXIII - Gestor de segurança da informação e comunicações: é o servidor público responsável pelas ações de segurança da informação e comunicações no ICMBio;
XXIV - Incidente: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;
XXV - Incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
XXVI - Informação: ativo que, como qualquer outro, é importante para os negócios, tem valor para a organização e, consequentemente, necessita ser adequadamente protegido, 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;
XXVII - Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
XXVIII - Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação;
XXIX - Perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;
XXX - Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
XXXI - Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;
XXXII - Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;
XXXIII - 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;
XXXIV - Segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, garantindo a continuidade de negociações, minimizando seu risco e maximizando o retorno sobre os investimentos e as oportunidades;
XXXV - Serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

XXXVI - Tratamento (processamento) da informação: recepção, produção, validação, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação, publicidade e controle da informação, inclusive as sigilosas;
XXXVII - Tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;
XXXVIII - Tempo Objetivo de Recuperação: é o tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente;
XXXIX - Usuário: agente público que obteve autorização do responsável pela área interessada para acesso aos ativos de Informação do ICMBio;
XL - Vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 5º 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 integridade: propriedade de que a informação não esteja modificada ou destruída de maneira não autorizada ou acidental;
III - a autenticidade: propriedade de que a informação seja produzida, expedida, modificada ou destruída por pessoa física, sistema, órgão ou entidade;
IV - 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;
V - a publicidade: dar transparência no trato da informação, observados os critérios legais;
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;
VII - a ética: os direitos dos agentes públicos devem ser preservados, sem o comprometimento da Segurança da Informação e Comunicações.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 6º As diretrizes de segurança da informação estabelecidas nesta POSIC aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo ICMBio, e que devem ser seguidas pelos agentes públicos, 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. 7º Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pelo ICMBio serão utilizados estritamente para seu propósito.
Parágrafo único. É vedado a qualquer agente público do ICMBio o uso dos recursos de Tecnologia da Informação e Comunicações 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.

Da Seção I
Da Gestão da Segurança da Informação e Comunicações

Art. 8º A Gestão da Segurança da Informação e Comunicações não se limita à tecnologia da informação e comunicações, compreendendo as ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos.
Art. 9º Toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas atividades no ICMBio, é considerada um bem e propriedade do Instituto e deve ser protegida segundo as diretrizes descritas nesta Política e demais regulamentações em vigor.

Seção II
Da Propriedade da Informação

Art. 10 A propriedade da informação será regida pelas seguintes diretrizes:
I - toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada por usuários que tenham acesso às informações do ICMBio, no exercício de suas atividades, é de propriedade desta entidade e será protegida segundo estas diretrizes e 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;
III - na cessão de bases de dados nominais custodiadas ou na informação de propriedade do ICMBio a terceiros, o gestor da informação providenciará a documentação formal relativa à autorização de acesso às informações.

Seção III
Da Classificação e Tratamento da Informação

Art. 11 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 ICMBio;

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 ICMBio;

Art. 12 Toda informação criada, manuseada, armazenada, transportada ou descartada do ICMBio será classificada de acordo com a Lei nº 12.527, de 18 de novembro de 2011.

Art. 13 As informações sob gestão do ICMBio 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 com o objetivo de limitar a exploração às informações exclusivas do Instituto.

Seção IV
Do Tratamento de Incidentes de Rede

Art. 14 A área de tecnologia da informação manterá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, instituída pelo Comitê de Segurança da Informação e Comunicações, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

Seção V
Da Gestão de Riscos

Art. 15 O Processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC - será implementado considerando, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do ICMBio e estará alinhado à metodologia denominada PDCA (Plan-Do-Check-Act), observando diretrizes e normas específicas no âmbito da Administração Pública Federal, de modo a fomentar sua melhoria contínua.

Seção VI
Da Gestão de Continuidade

Art. 16 As unidades descentralizadas do ICMBio devem manter processo de gestão de continuidade das atividades e serviços, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil, quando for o caso.

Art. 17 Aprovado pelo Comitê de Segurança da Informação e Comunicações, a área de tecnologia da informação do ICMBio deverá manter Plano de Contingências, gradado de acordo com o grau de probabilidade de ocorrência do evento ou sinistro, estabelecendo o conjunto de estratégias e procedimentos que devem ser adotados em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

Parágrafo único. As medidas constantes do Plano de Contingências devem minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

Seção VII
Do Monitoramento, Auditoria e Conformidade

Art. 18 O monitoramento, auditoria e conformidade observarão o seguinte:

I - o uso dos recursos de tecnologia da informação e comunicações disponibilizados pelo ICMBio é passível de monitoramento e auditoria e devem ser implementados e mantidos, sempre que possível, mecanismos que permitam a sua rastreabilidade;

II - a entrada e a saída de ativos de informação do ICMBio serão registradas e autorizadas por autoridade competente mediante procedimento formal;
III - A área de tecnologia da informação manterá registros e procedimentos, como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, à rede interna e à internet.

Seção VIII
Dos Controles de Acesso e Uso de Senhas

Art. 19 O controle de acesso e uso de senhas observará o seguinte:
I – o usuário que utiliza os recursos de TIC terá uma conta específica de acesso, pessoal e intransferível, conforme norma interna;
II - a autorização, o acesso, o uso da informação e dos recursos de tecnologia da informação e comunicações serão controlados e limitados ao cumprimento das atribuições de cada usuário, e qualquer outra forma de uso necessita de prévia autorização formal do gestor de cada setor ou unidade organizacional;
III - no caso de desvinculação temporária ou definitiva do usuário, os privilégios de acesso serão suspensos ou cancelados;
IV - os usuários serão orientados, de forma regular e periódica, a seguir as boas práticas de segurança da informação na seleção e uso de senhas.

Seção IX
Do Uso de e-mail

Art. 20 O correio eletrônico é um meio de comunicação corporativa do ICMBio.
§ 1º As regras de acesso e utilização de e-mail institucional devem atender às orientações desta POSIC, norma interna e demais diretrizes do Governo.
§ 2º A área de tecnologia deverá manter os controles do uso e cancelamento de acesso ao correio eletrônico.

Seção X
Do Acesso à Internet

Art. 21 O acesso à rede mundial de computadores - internet, no ambiente de trabalho, deverá ser regido por norma interna, atendendo esta POSIC e demais orientações governamentais e legislação em vigor.

Seção XI
Da Computação em Nuvem

Art. 22 O ICMBio poderá utilizar de tecnologias de Computação em Nuvem, desde que em conformidade com as diretrizes e normas específicas relacionadas à Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal.
Parágrafo único. Ao Gestor de Segurança da Informação e Comunicações, no âmbito de suas atribuições, cabe propor ações de segurança da informação e comunicações para a implementação ou contratação, no ICMBio, de tecnologias de computação em nuvem.

Seção XII
Do Uso, Aquisição, Desenvolvimento e Manutenção de Sistema de Informação

Art. 23 O uso, aquisição, desenvolvimento e manutenção de sistema de informação observarão as seguintes regras:
I – fica proibida permanentemente a instalação de quaisquer softwares sem licença de uso;
II - a área de Tecnologia da Informação do ICMBio fica autorizada a desinstalar todo e qualquer software sem licença de uso;
III - 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 ICMBio;
IV - o gerenciamento de mudanças deve incluir a garantia de que suas implementações sejam realizadas em horários apropriados, sem a perturbação dos processos de negócios cabíveis.
Art. 24 Cabe à área de Tecnologia da Informação do ICMBio, 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.

CAPÍTULO V
DAS PENALIDADES

Art. 25 O agente público responderá administrativa, civil e/ou penalmente pelo prejuízo que vier a ocasionar ao ICMBio, em decorrência do descumprimento das regras previstas nesta POSIC e demais normas internas e legislação vigente.

CAPÍTULO VI
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 26 A estrutura de Gestão de Segurança da Informação e Comunicações no ICMBio será composta pelo Gestor de Segurança da Informação e Comunicações (GSIC) e pelo Comitê de Segurança da Informação e Comunicações (CSIC).
Art. 27 O CSIC 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. 28 O CSIC realizará reuniões extraordinárias quando convocados pelo Gestor de Segurança de Informação e Comunicações.
Art. 29 Compete à Presidência do ICMBio, no âmbito da POSIC:
I - Promover cultura de segurança da informação e comunicações;
II - instituir Comitê de Segurança da Informação e Comunicações (CSIC);
III - nomear Gestor de Segurança da Informação e Comunicações;
IV - aprovar a POSIC e demais normas de segurança da informação e comunicações;
V - instituir a Equipe de Tratamento e Resposta a incidentes em redes computacionais;
VI - propor programa orçamentário específico para as ações de segurança da informação e comunicações;
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);

VIII - aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança.

Art. 30 Compete ao Gestor de Segurança da Informação e Comunicações do ICMBio:

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 - coordenar as ações de segurança da informação e comunicações;

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

VII - 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;

VIII - Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do ICMBio;

IX - Providenciar a divulgação interna desta POSIC.

Art. 31 Compete ao Comitê de Segurança da Informação e Comunicações (CSIC), no âmbito da POSIC:

I - Promover cultura de segurança da informação e comunicações;

II - Assessorar na implementação das ações de segurança da informação e comunicações no ICMBio;

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

IV - Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

CAPÍTULO VII
DA ATUALIZAÇÃO

Art. 32 Esta portaria deverá ser revisada e atualizada, no máximo, a cada três anos, a contar da data de sua publicação.

Art. 33 As áreas têm prazo de noventa dias, a contar da publicação desta POSIC, para submeterem ao Comitê de Segurança da Informação e Comunicações - CSIC proposta de atualização ou criação das normas internas complementares e específicas sobre segurança da informação e comunicações.

Art. 34 Esta portaria entra em vigor na data de sua publicação.

ROBERTO RICARDO VIZENTIN