RESOLUÇÃO CGD Nº 5, DE 06 DE MAIO DE 2020

Aprova versão atualizada da Política de Segurança da Informação e Comunicações do Ibama - POSIC, instituída por meio da Portaria nº 9, de 05 de junho de 2012.

O COMITÊ DE GOVERNANÇA DIGITAL DO INSTITUTO BRASILEIRO DO MEIO AMBIENTE E DOS RECURSOS NATURAIS RENOVÁVEIS - IBAMA, no uso da competência que lhe foi conferida pela Portaria nº 355, de 06 de fevereiro de 2020, publicada no Boletim de Serviço 02, de 07 de fevereiro de 2020, alterada pela Portaria nº 905, de 02 de abril de 2020, publicada no Boletim de Serviço 04, de 03 de abril de 2020,

CONSIDERANDO o constante dos autos do processo nº 02001.002849/2020-95,

RESOLVE:

Art. 1º Aprovar, na forma do anexo, versão atualizada da Política de Segurança da Informação e Comunicações do Ibama - POSIC, instituída por meio da Portaria nº 9, de 05 de junho de 2012.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

EDUARDO FORTUNATO BIM
Presidente do Comitê de Governança Digital

LUIS CARLOS HIROMI NAGAO
Diretor de Planejamento, Administração e Logística

CAROLINA FIORILLO MARIANI
Diretora de Qualidade Ambiental

JÔNATAS SOUZA DA TRINDADE
Diretor de Licenciamento Ambiental

OLÍMPIO FERREIRA MAGALHÃES
Diretor de Proteção Ambiental

JOÃO PESSOA RIOGRANDENSE MOREIRA JÚNIOR
Diretor de Uso Sustentável da Biodiversidade e Florestas

THIAGO ZUCCHETTI CARRION
Procurador-Chefe Nacional da Procuradoria Federal Especializada

MOSAR RODRIGUES RABELO JÚNIOR
Coordenador-Geral de Tecnologia da Informação

ANEXO I À RESOLUÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC) DO IBAMA

Seção I - Das Disposições Gerais

Art. 1º A Política de Segurança da Informação e Comunicações declara o comprometimento da alta direção organizacional com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação e comunicações no Ibama.

Seção II - Do Objetivo

Art. 2º Estabelecer direcionamentos, regras, objetivos e valores a serem adotados para a gestão de segurança da informação e comunicações em âmbito do IBAMA, de acordo com sua missão e com as leis e regulamentações relevantes ao caso. Para tanto, deve atender às seguintes orientações:

I - Estabelecer uma política clara e alinhada com a missão do IBAMA.

II - Obter apoio e comprometimento com a segurança da informação por meio da publicação, atualização e manutenção da POSIC - Política de Segurança da Informação e Comunicações para o IBAMA.

III - Revisar as diretrizes de segurança da informação a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Seção III - Dos Conceitos e Definições

Art. 3º Para fins da Política de Segurança da Informação e Comunicações considera-se:

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

II - Agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta.

III - Ameaça: causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização.

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

V - Aplicações: é um programa de computador que tem por objetivo ajudar o seu usuário a desempenhar uma tarefa específica, em geral ligada a processamento de dados;

VI - Avaliação de riscos: processo de análise de risco e avaliação de risco;

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

VIII - Ativos de informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

IX - Ciclo de vida: ciclo formado pelas fases da produção e recepção, organização, uso e disseminação e destinação;

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

XI - Colaborador: toda pessoa que se vincula ao Ibama, por meio de empresa prestadora de serviço ou por meio de contrato, convênio, acordo, ajuste ou outros instrumentos congêneres, tendo por finalidade a execução de atividades inerentes à Autarquia;

XII - Comitê de Segurança da Informação e Comunicação: 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);

XIII - Controle: meios de gestão de riscos, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, gerencial ou legal;

XIV - Evento: incidente ou ocorrência, a partir de fontes internas ou externas a uma entidade, capaz de afetar a realização dos seus objetivos;

XV - 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;

XVI - 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;

XVII - 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;

XVIII - Gestor de segurança da informação e informática: é responsável pelas ações de segurança da informação e comunicações no âmbito do Ibama;

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

XX - Impacto: alteração adversa do nível de objetivos de negócio alcançados;

XXI - 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;

XXII - 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;

XXIII - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXIV - Informação pessoal: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

XXV - Plano de Continuidade de Negócios – PCN: documentação dos procedimentos e informações necessárias para que o Ibama mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

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

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

XXVIII – Prestador de serviços: categoria composta por terceirizados contratados para execução de serviços específicos dentro das instalações do Ibama;

XXIX - Proprietário da informação: refere-se a parte interessada do Ibama, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência da informação;

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

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

XXXII - 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;

XXXIII - Segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXXIV - Segregação de Função: segregação de função é um método para reduzir o risco de mau uso, acidental ou deliberado dos ativos;

XXXV - Servidor Público: toda pessoa que se vincula ao Ibama, quer seja por meio de cargo, emprego ou função pública;

XXXVI - 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;

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

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

Seção IV - Dos Princípios

Art. 4º 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. 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 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; e

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 V - Do Objeto

Art. 6º As diretrizes de segurança da informação estabelecidas nesta POSIC aplicam-se às informações para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI) do Ibama, e que devem ser seguidas pelos agentes públicos da instituição e por todos os usuários que tenham acesso às suas informações, 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 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. 8º 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. 9º 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 VI - Das Diretrizes Gerais

Art. 10. No Ibama, 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 conforme norma complementar.(REDE CORPORATIVA E REDE INTERNA).

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

Art. 12. O cumprimento da política de segurança da informação e comunicações será auditado pela Auditoria do Ibama com a assessoria do Comitê de Governança Digital (CGD).

Art. 13. Os recursos de processamento da informação disponibilizados aos usuários terão suporte de um Plano de Prevenção de Riscos de acordo com a norma de Gestão de Riscos em segurança da informação a fim de evitar situações de risco à segurança da informação.

Art. 14. Quaisquer recursos de processamento da informação serão testados em ambiente de homologação antes de serem colocados em produção de acordo com norma de Aquisição Desenvolvimento e Manutenção de Sistemas.

Art. 15. Os servidores e colaboradores do Ibama estão sujeitos à POSIC – Política de Segurança da Informação e Comunicação e têm o dever de observar integralmente o disposto. A inobservância dessa política acarretará penalidades previstas no âmbito penal, civil e administrativo, na forma da legislação vigente.

Parágrafo único. Não é dado ao servidor ou colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicações, devendo este seguir rigorosamente o proposto. O desconhecimento desta política por parte do usuário não o isenta das responsabilidades e penalidades previstas.

Art. 16. É condição para acesso aos ativos de informação do Ibama a adesão formal aos termos desta Política.

Art. 17. O agente público do Ibama é responsável pela segurança dos ativos de informação e processos que estejam sob sua responsabilidade.

Parágrafo único. Ativos de tecnologia da informação e comunicação que necessitem de proteção adicional devido a sua criticidade e importância devem ser isolados e com controle restrito de acesso físico e lógico. O Ibama deve adotar ações de caráter preventivo para a contínua segurança e disponibilidade desses ativos de tecnologia da informação e comunicação.

Art. 18. Os gestores responsáveis pelos processos inerentes à gestão da segurança da informação receberão capacitação especializada de acordo com a norma de sensibilização, conscientização e capacitação em segurança da informação e comunicações.

Art. 19. Os contratos firmados pelo Ibama conterão cláusulas que determinem a observância desta política e das normas dela derivada

Parágrafo único. O Ibama deverá, em seus relacionamentos contratuais com terceiros, definir, especificamente, quais serviços e atividades serão autorizados para acesso e manuseio por terceiros. Deverá ser considerado, sempre, o menor perfil de privilégio para acesso às informações da Autarquia.

Art. 20. Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pelo Ibama serão utilizados estritamente para seu propósito.

Parágrafo único. É vedado, a qualquer colaborador e agente público do Ibama, 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 VII - Da Propriedade da Informação

Art. 21. Informação é patrimônio - Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IBAMA é considerada parte do seu patrimônio e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade.

I - toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada pelo colaborador e agente público do Ibama, 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 e de acordo com a norma de Classificação da Informação;

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 em seu TCI – Termo de Classificação da Informação;

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 em seu TCI – Termo de Classificação da Informação;

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 de acordo com a norma de aquisição desenvolvimento e manutenção de sistemas;

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

Parágrafo único. Os dados privados, pessoais e ou sensíveis do titular, de crianças e adolescentes devem ser processados de forma legal, justa e transparente em relação aos seus titulares.

Seção VIII - Da Classificação e Tratamento da Informação

Art. 22. 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. 23. 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. 24. 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);

II - 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 específica de classificação da informação.

Art. 25. 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 de acordo com a norma de classificação da informação;

Seção IX - Da Gestão de Incidentes de Segurança da Informação e Rede

Art. 26. 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. 27. Soluções de contorno aplicadas para minimizar a ocorrência de incidentes de segurança serão temporárias e imediatamente submetidas ao gestor de segurança da informação com definição do prazo para que a solução definitiva do problema seja implementada;

Art. 28. 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 tenha ocorrido.

Art. 29. A gestão de incidentes de segurança da informação deverá ser regida por norma complementar específica sobre a matéria.

Seção X - Do Gerenciamento de Riscos

Art. 30. As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicação – GRSIC deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do Ibama.

Art. 31. A abordagem de gestão de riscos estará alinhada ao processo de gestão de risco de todas as áreas do Ibama.

Art. 32. O processo de Gestão de Riscos de Segurança da Informação e Comunicação – GRSIC deve ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicação.

Art. 33. 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. 34. 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. 35. A gestão dos riscos em SIC terá como objetivo seu processo a fim de identificar as necessidades do Ibama em relação aos requisitos de Segurança da Informação e Comunicação, bem como, criar um sistema eficaz de Gestão de Segurança da Informação (SGSI).

Art. 36. O processo de gestão de riscos em SIC 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. 37. A gestão dos riscos em SIC seguirá os procedimentos definidos na Norma Complementar 04/IN01/DSIC/GSIPR de 14 de agosto de 2009.

Seção XI - Da Gestão de Continuidade de Negócio

Art. 38. O Ibama estabelecerá procedimentos a serem seguidos para minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

Art. 39. 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. 40. 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. 41. Toda informação institucional será mantida em local que a salvaguarde adequadamente.

Art. 42. As estratégias de continuidade deverão considerar o estudo dos tempos máximos de recuperação e restauração compatíveis com as necessidades dos processos de negócio.

I - RTO (Recovery Time Objective): compreende o tempo máximo que o negócio pode suportar sem a sua operacionalização;

II - RPO (Recovery Point Objective): compreende o ponto de recuperação dos dados, ou seja, uma vez recuperada a solução qual a quantidade de dados máxima que poderá ser perdida sem que o negócio seja afetado.

Art. 43. 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. 44. Os Planos serão testados periodicamente, coordenados pelo Comitê de Governança Digital CGD , de acordo com uma programação de testes.

Art. 45. A elaboração dos Planos de Continuidade do Negócio será realizada, preferencialmente, por uma equipe multidisciplinar, visando, que os planos sejam desenvolvidos com foco nos negócios ou nas atividades críticas.

Art. 46. O processo de gestão de riscos em Segurança da Informação com vistas a minimizar possíveis impactos associados aos ativos será definido em norma complementar (gestão de riscos em Segurança da Informação) específica sobre a matéria.

Seção XII - Do Monitoramento, Auditoria e Conformidade

Art. 47. A avaliação técnica de conformidade em Segurança da Informação e Comunicação deverá considerar a POSIC com suas normas e os requisitos legais pertinentes.

Art. 48. A avaliação de conformidade em SIC deve ser aplicada de forma contínua, visando contribuir para a Gestão de Segurança da Informação e Comunicação do CGD .

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; e

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.

Art. 49. A avaliação de conformidade de Segurança da Informação e Comunicação tomará como base, no mínimo, o inventário de ativos de informação, visando manter a disponibilidade, integridade, confidencialidade e autenticidade das informações.

Seção XIII - Do Controle de Acesso e Uso de Senhas

Art. 50. O controle de acesso e uso de senhas visa contribuir para a garantia da integridade, disponibilidade, confidencialidade e autenticidade das informações do Ibama e observará o seguinte:

I - Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Parágrafo único. Os servidores e os colaboradores do Ibama que utilizam os recursos de TIC terão uma conta específica de acesso, pessoal e intransferível, cuja concessão será regulamentada em norma complementar (a área de tecnologia da informação é responsável pela disponibilização do serviço).

II - O Ibama deve conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada.

§ 1º O Ibama deverá seguir o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;

§ 2º 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 e colaborador do Ibama, e qualquer outra forma de uso que necessita de prévia autorização formal do gestor de cada setor ou unidade organizacional;

§ 3º Sempre que houver mudanças nas atribuições de determinado colaborador ou agente público do Ibama, será de responsabilidade da chefia imediata solicitar a adequação imediata dos privilégios de acesso às informações e dos recursos de TIC;

§ 4º Os servidores e os colaboradores devem ser orientados a respeito dos procedimentos de segurança acerca do procedimento formal de registro, suspensão e bloqueio de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços;

§ 5º No caso de desvinculação temporária ou definitiva do agente público, os privilégios de acesso serão suspensos ou cancelados;

§ 6º Os servidores e os colaboradores serão orientados, de forma regular e periódica, a seguir as boas práticas de segurança da informação na seleção e uso de senhas conforme a norma de responsabilidades dos usuários;

§ 7º Os equipamentos devem ser utilizados única e exclusivamente por aqueles servidores e os colaboradores que assumirem a responsabilidade pelo seu uso;

§ 8º Os servidores e os colaboradores serão orientados a adotar uma política de "mesa limpa" e de "tela protegida" para reduzir os riscos de acesso não autorizado, perda e dano à informação, durante e fora do horário de trabalho;

§ 9º Os usuários receberão acesso somente a serviços que tenham sido especificamente autorizados a usar;

§ 10. Os métodos de autenticação de usuários nos sistemas garantirão autenticação segura, conforme norma complementar;

§ 11. Nas conexões advindas de localizações e equipamentos específicos serão implementadas identificações automáticas entre equipamentos como um meio de autenticar as conexões;

§ 12. O processo de log-on nos computadores / servidores de redes e sistemas de informação devem ser configurados com o intuito de se ter procedimento seguro;

§ 13. Os sistemas operacionais e aplicações disponibilizadas deverão ser configurados de maneira que os usuários tenham permissão alterar as suas próprias senhas de entrada no sistema (log-on), principalmente no primeiro acesso;

§ 14. Programas utilitários que possuam a capacidade de sobrepor os controles dos sistemas e aplicações serão de uso restrito e controlado; e

§ 15. Para os serviços e sistemas de informação considerados críticos deve haver mecanismos que limitem o horário e a origem da sua utilização.

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

Art. 51. O acesso à internet, uso de e-mail e outros recursos obedecerão ao seguinte:

I – As informações e os recursos de TI para acesso à rede do Ibama devem ser disponibilizados, única e exclusivamente, àqueles que os utilizam para o exercício de suas funções;

II – Todos os dispositivos utilizados para a proteção, manutenção da integridade, disponibilidade, e confidencialidade das informações devem ser considerados sigilosos, sendo, portanto, proibida a sua divulgação a pessoas não autorizadas ou a terceiros.

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

§ 2º As normas complementares deverão disciplinar o uso dos recursos e estar formalmente acompanhadas de um Termo de Responsabilidade (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 XV - Da Gestão de Ativos

Art. 52. A gestão de ativos deverá observar ao seguinte:

I – Os ativos associados à informação e aos recursos de processamento da informação devem ser identificados, e um inventário destes ativos seja estruturado e mantido;

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

§ 1º Cada um dos ativos identificados, será indicado um responsável (proprietário) e a classificação do ativo a ser identificado.

I - 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;

II - a eliminação de informações observará a norma complementar de procedimentos internos e classificação, e a temporalidade prevista na legislação (Conarq); e

III – Os ativos e os ativos de informação serão classificados de acordo com a classificação da informação armazenada, processada, manuseada ou protegida pelo ativo.

Seção XVI - Da Segurança Física dos Equipamentos

Art. 53. A segurança física dos equipamentos obedecerá ao seguintes:

I - A área responsável pela segurança organizacional/corporativa do Ibama deverá implementar perímetros de segurança a fim de garantir proteção e separação entre ambientes internos e externos;

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; e

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 XVII - Dos Serviços Terceirizados

Art. 54. Os serviços terceirizados seguirão ao seguinte:

I – O Ibama deverá, em seus relacionamentos contratuais com terceiros, definir, especificamente, quais serviços e atividades serão autorizados para acesso e manuseio por terceiros; e

II – Todo acesso por terceiros às informações e ativos do Ibama só serão autorizado após regular preenchimento de Termo de Responsabilidade pertinente de acordo com modelo na Política de Segurança da Informação e Comunicação (POSIC) do Ibama.

III - Toda atualização da POSIC do Ibama bem como de procedimentos, sistemas e processos envolvidos deverão ser repassados a terceiros contratados a fim de se manter alinhado o conhecimento e implementação de mudanças de segurança necessárias à Autarquia.

Seção XVIII - Do Planejamento e Aceitação dos Sistemas

Art. 55. O planejamento e aceitação dos sistemas do Ibama seguirão ao seguinte:

I – O Ibama estabelecerá exigências acerca da segurança afeta as aplicações adquiridas;

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

III – O Ibama solicitará e receberá todos os códigos-fontes e direitos de propriedade intelectual as aplicações adquiridas;

IV – Implementar testes para aplicações a fim de se comprovar que erros, falhas e vulnerabilidades foram, efetivamente, evitados dentro do ciclo de desenvolvimento dessas soluções;

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

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 (gerenciamento da segurança em redes);

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; e

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 (NTP).

Art. 56. 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 XIX - Do Uso, Aquisição, Desenvolvimento e Manutenção de Sistema de Informação

Art. 57. 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 solicitar 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 – Solicitar prévia aprovação técnica e conter regras de segurança a fim de se manter protegida as informações veiculadas por essas soluções;

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 – Solicitar e receber todos os códigos-fontes e direitos de propriedade intelectual das aplicações adquiridas;

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

XI - O gerenciamento de mudança deverá incluir:

§ 1º a manutenção de um registro dos níveis acordados de autorização;

§ 2º controlar todas as mudanças realizadas em aplicações e sistemas operacionais;

§ 3º a análise crítica dos procedimentos de controle e integridade para assegurar que as mudanças não os comprometam;

§ 4º segurança necessária para autenticação, autorização e acesso a suas bases de dados;

§ 5º a obtenção de aprovação formal para propostas detalhadas antes da implementação;

§ 6º a garantia da aceitação das mudanças por usuários autorizados, antes da implementação;

§ 7º a garantia da atualização da documentação do sistema após conclusão de cada mudança e de que a documentação antiga seja arquivada;

§ 8º a manutenção de um controle de versão de todas as atualizações de softwares;

§ 9º a manutenção de uma trilha para auditoria de todas as mudanças solicitadas;

§ 10. a garantia de que toda a documentação operacional e procedimentos dos usuários sejam alterados conforme necessário e que se mantenham apropriados; e

§ 11. 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. 58. 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. 59. As regras específicas de operação e manutenção em sistemas considerados críticos no Ibama serão definidas em norma complementar (aquisição desenvolvimento e manutenção de sistemas); e

Art. 60. As regras específicas de operação e manutenção em soluções de Tecnologia da Informação e Comunicação serão definidas em norma complementar.

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

Art. 61. 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 XXI - Da Gestão de Segurança na Comunicação

Art. 62. 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 norma da organização interna da segurança da informação e comunicação da POSIC – Politica de Segurança da Informação e 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; e

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

Art. 63. As regras específicas da segurança na comunicação do Ibama serão estabelecidas em norma complementar.

Seção XXII - Da Gestão de Recursos Humanos

Art. 64. A gestão de Recursos Humanos observará ao seguintes:

I - os acessos dos servidores públicos aos sistemas corporativos ou aos sistemas disponibilizados ao Ibama deverão ser regulamentados, conforme norma complementar (Procedimentos e responsabilidades operacionais); e

II - os prestadores de serviço do Ibama deverão conhecer e cumprir a Política de Segurança da Informação e Comunicações (POSIC).

Art. 65. As regras específicas da segurança de gestão de recursos humanos do Ibama serão definidas em norma complementar (Recursos humanos).

Seção XXIII - Da Proteção de Dados Pessoais

Art. 66. Os dados privados, pessoais e ou sensíveis do titular, de crianças e adolescentes deverão ser processados de forma legal, justa e transparente em relação aos seus titulares e observará os seguintes:

I – Devem ser coletados para fins específicos, explícitos e legítimos e não processados posteriormente de maneira incompatível com esses objetivos;

II – Devem estar adequados, relevantes e limitados ao uso necessário e em relação aos fins para os quais são destinados e/ou processados;

III – Quando solicitado pelo titular e/ou quando necessário, os dados devem ser atualizados;

IV – Os dados pessoais devem ser armazenados por períodos mais longos, desde que os dados pessoais sejam processados exclusivamente para arquivamento no interesse público, para fins de pesquisa científica ou histórica ou para fins estatísticos sujeitos à implementação das medidas técnicas e organizacionais apropriadas exigidas pela Lei 13.709 – LGPD;

V – Deve-se ter cuidado no tratamento de dados pessoais/privados sensíveis; e

VI – As atribuições e responsabilidades do profissional responsável e/ou encarregado (DPO) pela proteção de dados pessoais/privados e informações sensíveis será exercida pelo Gestor de Segurança da Informação.

Seção XXIV - Das Competências e Responsabilidades

Art. 67. A estrutura de Gestão de Segurança da Informação no Ibama será composta pelo Gestor de Segurança da Informação (GSI) e pelo Comitê de Governança Digital CGD.

Art. 68. O gestor de Segurança da Informação do Ibama será precipuamente o Presidente da autarquia, podendo indicar para a função membro do Comitê de Governança Digital CGD que ocupe cargo em comissão ou função de confiança de nível 5 ou superior do Grupo-Direção e Assessoramento Superiores ou equivalente .

Art. 69. O Comitê de Governança Digital CGD deverá realizar reuniões periódicas para acompanhamento das atividades de segurança institucional, avaliação do cumprimento de metas de segurança e a efetiva aplicação dessa POSIC.

Art. 70. O Comitê de Governança Digital CGD deverá criar Grupos de Trabalho para realizar as seguintes atividades:

I - manter contato permanente com o Departamento de Segurança da Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República GSI/PR, sob supervisão do Gestor de Segurança da Informação - GSI;

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

III - realizar outras atividades relacionadas às suas atribuições.

Art. 71. 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 Governança Digital CGD ;

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. 72. São competências do Comitê de Governança Digital CGD :

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.

Art. 73. São competências do Gestor de Segurança da Informação:

I - presidir o Comitê de Governança Digital CGD , na ausência do Presidente, quando a pauta for relativa a segurança da informação e comunicações;

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 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 direto com o Departamento de Segurança da Informação e Comunicações - DSIC 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; e

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

Art. 74. São responsabilidades atribuídas aos usuários que utilizam os recursos de processamento pertencentes ou controlados pelo Ibama:

I - conhecer e cumprir a POSIC - Política de Segurança da Informação 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 CGD ; e

VI - participar de eventos promovidos pelo CGD relacionados à segurança de informação.

Art. 75. 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 XXV - Das Penalidades

Art. 76. 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 XXVI - Das Disposições Finais

Art. 77. 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. 78. Os casos omissos serão resolvidos pelo Comitê de Governança Digital CGD.

Art. 79. Este documento entra em vigor a partir da data de sua publicação e pode ser atualizado ou cancelado pela ocorrência de alguma das seguintes situações:

I - Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma; e

II - Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento.

Art. 80. A aprovação e divulgação da norma alterada seguirá o mesmo processo de elaboração, tendo como condições obrigatórias de atualização do documento:

I - Surgimento ou alteração de leis e/ou regulamentações vigentes;

II - Mudança estratégica da instituição que tenha impacto nesta Norma;

III - Mudança de tecnologia no Ibama que tenha impacto nesta Norma; ou

IV - A partir dos resultados das análises de riscos realizadas no Ibama que venham a impactar/provocar necessária mudança em normativo de segurança para readequação da Autarquia aos riscos encontrados (mitigação).