Comitê de Governança Digital

Resolução CGD nº 8, de 26.11.2021

Aprova versão atualizada da Política de Segurança da Informação e Comunicações do Ibama - POSIC.

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, e atualizações. CONSIDERANDO o constante dos autos do processo nº 02001.002849/2020-95. R E S O L V E :

Art. 1º Aprovar, na forma do anexo, versão atualizada da Política de Segurança da Informação e Comunicações do Ibama - POSIC, instituída por meio da Resolução CGD Ibama nº 05, de 06 de maio de 2020, publicada no Boletim de Serviço Especial 05A, de 15 de maio de 2020.

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

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES POSIC

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 possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

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

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

V - 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 comparar o risco estimado com critérios de risco predefinidos para determinar a importância do 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 no âmbito do órgão ou entidade da APF, no Ibama suas funções foram absorvidas pelo

Comitê de Governança digital;

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

XIV - Evento: qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança;

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: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

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: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

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

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: documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SI (Este termo substituiu o termo Política de Segurança da Informação e Comunicações); XXVIII - Prestador de serviços: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso físico ou remoto;

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.

Parágrafo único. Vale o Glossário de Segurança da Informação, aprovado pelo Gabinete de

Segurança Institucional da Presidência da República por meio da Portaria GSI/PR nº 93, de 26 de setembro de 2019, como referência na elaboração de normativos internos afetos à segurança da informação e de trabalhos correlatos.

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.

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

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

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

I – 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.

II - 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 nº

13.709, de 14 de agosto de 2018 – 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), pelo Comitê de Governança Digital CGD e pela Equipe de Tratamento de Incidentes em Redes Computacionais (Etir).

Art. 68. O gestor de Segurança da Informação do Ibama deverá ser escolhido dentre os membros do Comitê de Governança Digital que ocupe cargo efetivo de carreira do Ibama.

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 - acompanhar os trabalhos da Equipe de Tratamento de Incidentes em Redes

Computacionais (Etir);

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 do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação;

IX - coordenar a gestão de riscos em segurança da informação realizada no Ibama; X - propor normas relativas à segurança da informação e comunicações;

X - 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); XI - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de

Segurança Institucional da Presidência da República;

XII - assessorar a alta administração na implementação da Política de Segurança da Informação; XIII - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

XIV - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

XV - propor recursos necessários às ações de segurança da informação;

XVI - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação; e

XVII - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação.

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).

Resolução CGD Nº 9, de 26.11.2021

Aprova versão atualizada das Normas Complementares de Segurança da Informação e Comunicações do Ibama.

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, e atualizações. CONSIDERANDO o constante dos autos do processo nº 02001.002849/2020-95. R E S O L V E :

Art. 1º Aprovar, na forma dos anexos, versão atualizada das seguintes Normas Complementares de Segurança da Informação e Comunicações do Ibama.

I. Norma Complementar 02 - Procedimentos de acesso, consulta, alteração, monitoramento e gerenciamento de sistemas de informação do Ibama

II. Norma Complementar 05 - Uso e administração do sistema de correio eletrônico

III. Norma Complementar 06 - Gestão de Riscos de Segurança da Informação

IV. NC 07 - Uso de Internet, Intranet e Extranet

V. NC 08 - Classificação de Documentos Sigilosos

VI. NC 09 - Uso de auditórios e salas do Ibama para o serviço de videoconferência

VII. NC 10 - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR

VIII. NC 11 - Gestão de continuidade de negócios - 11140551

IX. NC 12 - Gestão dos serviços terceirizados

X. NC 13 - Processo de Gestão de Riscos de Segurança da Informação

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

ANEXO I
Norma Complementar 02

	Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis		
Número da Norma	Revisão	Emissão	Folha
02/NC/POSIC/CGD	02	03/11/2	1

ORIGEM

		021	
Procedimentos de acesso, consulta, alteração, monitoramento e gerenciamento de sistemas de informação do Ibama, no âmbito da Política de Segurança daInformação, Informática e Comunicações - POSIC			

Comitê de Governança Digital do Ibama (CGD)

- Instrução Normativa 01 GSI/PR, de 27 de maio de 2020;

REFERÊNCIA NORMATIVA

- ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão da Segurança da Informação;
- ABNT ISO/IEC 27002:2013 – Código de Prática para Controles de Segurança da Informação;
- Norma Complementar n° 07/IN01/DSIC/GSIPR – Diretrizes para Implementação de Controles de Acesso relativos à Segurança da Informação e Comunicações;
- Norma Complementar n° 16/IN01/DSIC/GSIPR – Diretrizes para Desenvolvimento e Obtenção de Software Seguro; e Decreto nº 9.637/2018.

CAMPO DE APLICAÇÃO

Esta Norma Complementar substitui a NC 02/NC/POSIC/CSII, de 08/08/2014.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta Norma Complementar substitui a NC 02/NC/POSIC/CSII, de 08/08/2014.

APROVAÇÃO

_____

Presidente do Ibama

Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma	Revisão	Emissão	Folha
02/NC/POSIC/CGD	02	03/11/2021	2
Procedimentos de acesso, consulta, alteração, monitoramento e gerenciamento de sistemas de informação do Ibama, no âmbito da Política de Segurança daInformação, Informática e Comunicações - POSIC			

1 OBJETIVO

Regulamentar os procedimentos de segurança para acesso, senhas, consulta, alteração, monitoramento e gerenciamento de sistemas de informação do Ibama, no âmbito da Política de Segurança da Informação, Informática e Comunicações do Ibama - POSIC.

2 CONCEITOS E DEFINIÇÕES

Para o entendimento adequado desta norma, em conformidade com a POSIC, considera-se:

2.1 Acesso – ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

2.2 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;

2.3 Autenticação de multifatores (MFA) – utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito);

2.4 Biometria – verificação da identidade de um indivíduo por meio de uma característica física ou comportamental única, através de métodos automatizados;

2.5 Bloqueio de acesso – processo que tem por finalidade suspender temporariamente o acesso;

2.6 Conta de serviço – conta de acesso à rede corporativa de computadores necessária a um procedimento automático (aplicação, script, etc.) sem qualquer intervenção humana no seu uso;

2.7 Controle de acesso – - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais.

2.8 Via de regra, requer procedimentos de autenticação;

2.9 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;

2.10 Credencial (ou conta de acesso) – permissão, concedida por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha);

2.11 Exclusão de acesso – processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso;

2.12 Perfil de acesso – conjunto de atributos de cada usuário, definidos previamente como

necessários para credencial de acesso;

2.13 Quebra de segurança – ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações.

2.14 Sistema de acesso – conjunto de ferramentas que se destina a controlar e a dar permissão de acesso a uma pessoa a um recurso;

2.15 Sistema biométrico – conjunto de ferramentas que se utilizadas características de uma pessoa, levando em consideração fatores comportamentais e fisiológicos, a fim de identificá-la de forma unívoca;

2.16 Termo de responsabilidade – termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

2.17 Tratamento da informação – conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

2.18 Usuário – pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da APF, formalizada por meio da assinatura de Termo de Responsabilidade;

3 DIRETRIZES

3.1 O acesso lógico ao sistema de informação do Ibama deverá empregar os seguintes métodos de autenticação de usuário:

3.1.1 Autenticação de usuário com mais de um fator – autenticação de múltiplos fatores – sempre que possível; e

3.1.2 No mínimo, autenticação com certificação digital para gestores, operadores administrativos e perfis críticos de acesso, conforme legislação em vigor.

3.2 Os sistemas de informação do Ibama devem conter um conjunto de processos de negócio e de mecanismos lógicos e físicos capazes de viabilizar, quando necessário, trilhas de auditoria aos controles de acesso, principalmente, no tocante ao uso e manutenção das identidades digitais, conforme Norma Complementar nº 07 e IN01/DSIC/GSI/PR.

3.3 Os sistemas de informação do Ibama que tratam informações sigilosas e aqueles relacionados à liberação ou manipulação de recursos públicos devem implementar trilhas de auditoria, conforme legislação em vigor.

3.4 A criação de contas de acesso aos sistemas do Ibama requer procedimentos prévios de credenciamento para todos os usuários.

3.5 Deverá ser disponibilizada ao usuário, que não exerce funções de administração da rede local, somente uma única conta institucional de acesso, pessoal e intransferível.

3.6 Poderá ser utilizada conta de acesso no perfil de administrador somente por usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

3.7 A senha é de uso pessoal e intransferível do usuário, que deve mantê-la em sigilo. O usuário não poderá compartilhar a sua senha pessoal com terceiros em nenhuma hipótese.

3.8 O usuário deverá utilizar uma senha forte. Senhas fortes são difíceis de serem descobertas, com no mínimo oito caracteres, formadas por uma combinação de números, caracteres, maiúsculos, minúsculos e especiais.

3.9 O usuário que perceber de alguma forma que a sua senha pessoal tenha sido copiada, roubada ou divulgada deverá imediatamente alterá-la.

3.10 Será solicitada a alteração da senha a cada 06 (seis) meses, e ao usuário não será permitido utilizar as 03 (três) senhas anteriores.

3.11 Os sistemas do Ibama que têm habilitado o uso da certificação digital deverão ser acessados por meio de tokens, com a sua respectiva senha.

3.12 A conta dos agentes públicos do Ibama poderá ser desabilitada nas seguintes situações:

3.12.1 Quando permanecer inativa por mais de 60 dias, sem justificativa prévia;

3.12.2 Quando o usuário for cedido a outro órgão;

3.12.3 Quando o contrato de trabalho de terceirizados e de servidores de contratos temporários for encerrado;

3.12.4 Por descumprimento das normas de segurança;

3.12.5 Por erros recorrentes de combinação de usuário e/ou senha no momento de login em sistemas e computadores, de no máximo cinco tentativas.

3.13 A concessão de autorização de acesso aos sistemas de informação pelos agentes públicos está condicionada ao aceite do termo de ciência das suas normas.

3.14 Os pedidos de credenciamento, de descredenciamento e de mudança do nível de permissão de acesso de usuários internos aos sistemas de informação do Ibama devem ser realizados formalmente pela chefia imediata, ou por autoridade de mesmo nível ou superior, ao gestor do sistema, detalhando os acessos e privilégios necessários.

3.15 É vedado o uso dos sistemas de informação do Ibama por servidores inativos, na condição de usuário interno.

3.16 O acesso de terceirizados, fornecedores e prestadores de serviços será expressamente solicitado pelo respectivo Diretor ou Superintendente e autorizado pelo gestor do sistema.

3.17 Todos os agentes públicos do Ibama deverão utilizar obrigatoriamente a certificação digital para acessar os sistemas de informação do Ibama que já possuem essa tecnologia.

3.17.1 É de responsabilidade do Ibama fornecer a certificação digital aos seus servidores efetivos, de contrato temporário, ocupantes de cargo comissionado e estagiários.

3.17.2 O fornecimento de certificado digital aos profissionais vinculados a outras empresas, organizações ou instituições que prestam serviços ao Ibama, tais como procuradores federais e servidores em exercício descentralizado, agentes públicos de outras instituições, terceirizados e outros, correrá às expensas das respectivas empresas, organizações ou instituições.

3.18 O acesso de pessoal terceirizado para realização de trabalhos de manutenção de equipamentos dos sistemas de informação deverá ser acompanhado por servidor do Ibama.

3.19 A concessão de autorização de acesso aos sistemas de informação do Ibama a usuários externos é condicionada ao aceite do termo de ciência das suas normas.

3.20 Fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União.

3.21. Deverão ser observadas as diretrizes do art. 3° do Decreto n° 10.046/2019 e o disposto na Lei n° 13.709/2019 (LGPD).

3.22 O acesso restrito aos sistemas de informação do Ibama será autorizado pelo gestor administrador do sistema mediante procedimento próprio.

3.23 O acesso a dados corporativos do Ibama pelas instituições parceiras somente será permitido mediante autorização expressa do Presidente do Ibama.

3.24 Para o controle de acesso aos sistemas de informação do Ibama, são adotadas as seguintes premissas:

3.24.1 Quando houver restrição ao acesso, este deve ser monitorado;

3.24.2 A liberação de acesso aos sistemas de informação deve ser precedida de treinamento ou orientação, de acordo com o contexto e o perfil de cada usuário.

3.25 O monitoramento dos sistemas de informação do Ibama tem como objetivo prover o funcionamento permanente e seguro desses sistemas, de modo a garantir a disponibilidade, a continuidade, a integridade e, quando couber, o sigilo dos dados, das informações e dos documentos e, ainda, detectar atividades não autorizadas e eventuais falhas.

3.26 A Coordenação-geral de Tecnologia da Informação - CGTI deverá adotar os seguintes procedimentos:

3.26.1 Monitoramento e controle dos sistemas de informações do Ibama;

3.26.2 Auditoria dos registros de acesso para identificação de vulnerabilidades e de uso indevido dos sistemas de informação do Ibama.

3.27 A CGTI poderá determinar a suspensão de todos os acessos dos usuários aos sistemas quando houver indícios de violação do disposto neste regulamento, a fim de evitar dano ou comprometimento dos sistemas de informação.

3.27.1 A autoridade máxima da unidade na qual haja agente público respondendo a inquérito policial, sindicância ou processo administrativo disciplinar, solicitará à CGTI a restrição de acesso aos sistemas de informação do Ibama, assim que tomar conhecimento do fato.

3.28 Os indícios de prática de procedimentos que possam ocasionar quebra de segurança ou violação das disposições constantes desta Norma deverão ser comunicados ao Comitê de Governança Digital - CGD do Ibama, para análise e encaminhamento.

3.29 A conta de acesso biométrico, quando implementada, deve ser vinculada à conta de acesso lógico, a fim de atender os conceitos da autenticação de multifatores.

3.30 O órgão ou entidade deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

4 RESPONSABILIDADES

4.1 A Coordenação-geral de Tecnologia da Informação - CGTI é responsável pelo desenvolvimento de ações que visem à implementação e ao gerenciamento de medidas e

procedimentos de segurança previstos nesta norma e pelo provimento de apoio técnico ao Comitê de Governança Digital - CGD do Ibama.

4.2 Os gestores dos sistemas serão responsáveis pelos procedimentos autorizativos de acesso aos sistemas, que serão normatizados em atos administrativos específicos.

4.3 Todo usuário, no âmbito de suas competências, deve zelar pela segurança da informação contida no sistema.

4.4 É proibida a cópia ou a captação não autorizada, por qualquer modo ou meio, de qualquer arquivo ou ativo proveniente de sistemas de informação do Ibama de acesso restrito.

4.5 Os responsáveis pelos serviços dos ativos informacionais do Ibama devem comunicar oficial e imediatamente ao Gestor de Segurança da Informação, para fins de acompanhamento e providências, qualquer caso de suspeita de ilícito ou de ameaça à segurança dos sistemas.

5 DISPOSIÇÕES GERAIS

5.1 O desligamento de agentes públicos que forem usuários de sistemas de informação do Ibama deve ser comunicado pela chefia imediata aos gestores dos respectivos sistemas, devendo ser formalmente solicitado o descredenciamento dos agentes, conforme previsto no item 3.14 desta Norma.

5.2 Em caso de desligamento de terceirizados com acesso autorizado aos sistemas de informação do Ibama e à rede, a chefia imediata deverá solicitar à CGTI o seu descredenciamento.

5.3 As regras dispostas na presente Norma aplicam-se tanto a agentes públicos do Ibama – servidores, terceirizados, estagiários e ocupantes de cargos comissionados – como a usuários externos.

5.4 Os usuários externos serão informados das regras previstas no *caput* por meio do aceite de que trata o item 3.19 desta Norma.

5.5 Os casos omissos e as dúvidas a respeito desta Norma serão submetidos ao Comitê de Governança Digital - CGD e à Coordenação-geral de Tecnologia da Informação - CGTI.

6 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO II
Norma Complementar 05

	Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis		
Número da Norma	Revisão	Emissão	Folha
05/NC/PO-SIC/CGD	01	20/10/2021	1

Uso e administração do sistema de correio eletrônico do Ibama, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC

ORIGEM

Comitê de Governança Digital do Ibama (CGD)

REFERÊNCIA NORMATIVA

- Instrução Normativa GSI/PR nº 1, de 27.05.2020;
- Instrução Normativa GSI/PR nº 2, de 24 de julho de 2020;
- Norma Complementar nº 01/IN01/DSIC/GSIPR, de 15.10.2008;
- ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão da Segurança da Informação; e
- ABNT ISO/IEC 27002:2013 – Código de Prática para Controles de Segurança da Informação.

CAMPO DE APLICAÇÃO

Esta norma aplica-se no âmbito do Ibama.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta Norma Complementar substitui a NC 05/NC/POSIC/CSII, de 28/12/2012.

ANEXO II

IBAMA MMA	**Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis**		
Número da Norma	REVISÃO	Emis- são	FOLHA
05/NC/PO SIC/CGD	0 1	20/10/2 021	1
Uso e administração do sistema de correio eletrônico do Ibama, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

1 CONSIDERAÇÕES INICIAIS

O correio eletrônico, serviço provido pela Coordenação-geral de Tecnologia da Informação - CGTI, possui como finalidade permitir a troca de informações relacionadas às atividades deste Instituto, que abrange a Sede e suas Unidades descentralizadas, sendo seu uso e administração regulamentados pela presente Norma.

2 CONCEITOS E DEFINIÇÕES

Para os fins desta norma, considera-se:

2.1 Armazenamento local: repositório de dados, sob gestão direta do usuário, como arquivos de pastas particulares, nos quais podem ser armazenados itens de correio eletrônico, quando instalado um cliente de e-mail no computador do usuário;

2.2 Caixa postal ou caixa de correio eletrônico: repositório de dados associado a um endereço de correio eletrônico, de capacidade definida e destinada ao armazenamento de mensagens eletrônicas;

2.3 Caixa de correio eletrônico individual funcional: caixa de correio de uso individual, isto é, está associada a uma única pessoa, por meio de um endereço de correio eletrônico;

2.4 Caixa de correio eletrônico de uma unidade organizacional do Ibama: caixa de correio eletrônico designada para uso pelas unidades organizacionais do Ibama com, obrigatoriamente, pelo menos um responsável pelo seu gerenciamento e manutenção;

2.5 Cliente de e-mail: programa de computador utilizado para o gerenciamento de correio eletrônico;

2.6 Endereço de correio eletrônico: identificação digital única, em conformidade com a RFC 821 - Simple Mail Transfer Protocol - SMTP;

2.7 Endereço de correio eletrônico do Ibama: endereço de correio eletrônico pertencente a qualquer domínio do Ibama. Exemplo: @ibama.gov.br;

2.8 E-mail: conjunto de informações em formato digital, encapsuladas em um invólucro virtual, no qual consta, no mínimo, o endereço de correio eletrônico do remetente e de, pelo menos, um destinatário;

2.9 Lista ou grupo de discussão: ferramenta que permite a um grupo de pessoas a troca de mensagens via e-mail entre todos os membros do grupo;

2.10 Serviço de correio eletrônico: conjunto de recursos computacionais que permitem o envio e o recebimento de e-mails, bem como seu armazenamento em caixas postais;

2.11 Usuários especiais: usuários que ocupam cargo de confiança, servidores cedidos por outros órgãos, pessoas vinculadas a empresas prestadoras de serviços ao Ibama, consultores contratados para trabalhar em projetos no Ibama e estagiários.

3 DIRETRIZES

3.1 As informações contidas na caixa postal são de propriedade do Ibama.

3.2 As informações da caixa postal são passíveis de auditoria, monitoramento e controle.

3.3 As caixas postais individuais funcionais do Ibama seguirão, a Norma de Formação de Nomes dos endereços eletrônicos (e-mail), com base na padronização aprovada pelo Governo Federal, conforme a Norma GOV.BR ePING (https://www.gov.br/governodigital/pt-br/governanca-de-dados/padrao-de-formacao-de- enderecos-de-correio-eletronico.pdf).

3.4 Os usuários devem utilizar o e-mail institucional para as comunicações de caráter institucional, sendo vedado o uso de e-mails de outros provedores desse tipo de serviço para essas comunicações.

3.4.1 Todo servidor do Ibama possuirá uma caixa de correio eletrônico individual funcional para comunicação institucional.

3.4.2 Os usuários deverão aceitar o Termo de Responsabilidade do uso de e-mail do Ibama no momento de seu primeiro acesso ao e-mail.

3.4.3 As caixas de correio poderão ser acessadas por seus titulares de modo remoto, a partir de equipamentos externos à rede local do Ibama.

3.5 Compete à CGTI o estabelecimento de limites operacionais ao sistema de correio eletrônico de modo a garantir seu pleno funcionamento, de maneira continua e ininterrupta.

3.5.1 Compreendem tais limites os seguintes aspectos:

3.5.1.1 Espaço físico destinado às caixas postais;

3.5.1.2 Tamanho máximo de mensagens, compreendendo cabeçalho, texto e anexos;

3.5.1.3 Número máximo de destinatários para cada mensagem a ser enviada.

3.5.2 A capacidade de cada caixa postal é determinada pelo tipo de usuário que a utiliza e a sua finalidade.

3.6 Para o gerenciamento do espaço físico de armazenamento destinado às caixas postais, serão adotados os seguintes procedimentos:

3.6.1 Sempre que o limite de armazenamento da caixa postal estiver próximo a ser atingido, a caixa postal exibirá um alerta indicativo;

3.6.2 Apenas serão entregues as mensagens que não ultrapassarem o espaço livre disponível na caixa postal do usuário;

3.6.3 Será enviada, imediatamente, uma notificação ao remetente, informando que a mensagem original não foi entregue ao destinatário devido à falta de espaço na caixa postal deste.

3.7 A caixa postal individual funcional será considerada inativa e será bloqueada no sistema de correio eletrônico, tornando-se inacessível ao usuário, caso ocorra uma das seguintes situações:

3.7.1 Transcurso de trinta dias sem qualquer acesso;

3.7.2 Término do vínculo com o Ibama;

3.7.3 Aposentadoria do servidor;

3.7.4 Usuário especial desligado do Ibama.

3.8 A utilização de um cliente de e-mail instalado pela Equipe de Suporte de Informática do Ibama Sede e pelos Núcleos de Informática nas Superintendências Estaduais proverá o meio de exportar as mensagens periodicamente, a fim de liberar espaço no servidor de e-mails para o recebimento de novas mensagens.

3.9 A caixa postal será considerada como caixa de um endereço de correio eletrônico institucional nos seguintes casos:

3.9.1 Quando estiver associada a uma unidade organizacional do Ibama, por meio de um endereço de correio eletrônico;

3.9.2 Quando estiver associada diretamente a um projeto;

3.9.3 Quando estiver vinculada a aplicações computacionais específicas ou ao próprio sistema de correio eletrônico.

3.10 A solicitação para a criação da caixa postal institucional deverá ser encaminhada à CGTI, por meio de ofício do chefe imediato ou do titular da unidade ao qual o responsável.

3.10.1 Toda caixa postal institucional deverá ter um usuário responsável, em caso de necessidade de contato.

3.10.2 O responsável pela caixa institucional poderá delegar a outras pessoas a manutenção da caixa postal, desde que supervisione a sua utilização.

3.10.3 A caixa postal institucional é independente da caixa postal de seu responsável, tanto no acesso quanto no espaço de armazenamento.

3.10.4 A criação da caixa postal institucional, prevista no item 3.9.2 será providenciada pela CGTI, no momento do lançamento do projeto.

3.10.5 As caixas de correio eletrônico institucionais poderão ser acessadas remotamente pelos usuários autorizados, a partir de equipamentos não conectados à rede local do Ibama.

3.11 Caso ocorra extinção da unidade organizacional à qual a caixa institucional estiver relacionada, caberá à instância hierarquicamente superior decidir sobre as ações a serem tomadas sobre a caixa de correio e seu conteúdo.

3.12 A caixa postal institucional será considerada inativa caso ocorra o transcurso de seis meses sem

qualquer acesso.

3.13 As caixas de correio institucionais previstas no item 3.9.2 serão designadas como caixas postais de projetos.

3.13.1 Imediatamente após o término da execução do projeto, a unidade responsável pelo projeto deverá solicitar à CGTI a desativação de sua caixa postal.

3.13.2 Após a oficialização do término do projeto, a caixa postal será mantida ativa por um período de até 90 (noventa) dias, designado como período de transição.

3.13.3 No período de transição indicado no item 3.13.2, a unidade responsável pelo projeto poderá solicitar:

3.13.3.1 A geração de cópia em meio digital de todas as mensagens até então armazenadas;

3.13.3.2 A ativação do serviço de resposta automática para as mensagens encaminhadas à caixa postal do projeto informando-se o conteúdo desejado;

3.13.3.3 O encaminhamento automático ("forward") das mensagens recebidas para uma outra caixa postal indicada pelo seu responsável mediante solicitação expressa.

3.14 A solicitação para a criação de uma lista de discussão deverá ser encaminhada à CGTI, por meio de ofício do chefe imediato ou do titular da unidade ao qual o responsável pelo gerenciamento da lista estiver subordinado.

3.14.1 A solicitação de criação de uma lista de discussão deverá conter a sua necessidade justificada.

3.14.2 As listas de discussão poderão ter mais de um responsável, ficando essa atribuição a critério do solicitante.

3.15 O envio de mensagens para a lista de discussão será restrito aos usuários previamente autorizados pelo responsável pela lista, que fará a sua moderação.

3.16 Até o final do primeiro trimestre de cada ano, a equipe de administradores do correio eletrônico providenciará a exclusão das listas de discussão consideradas inativas.

3.17 A CGTI observará o sigilo das comunicações, abstendo-se de qualquer ação que implique a violação de mensagem com o objetivo de conhecer ou divulgar seu conteúdo.

3.17.1 Em manutenções necessárias à solução de problemas técnicos que afetem o funcionamento normal do sistema, as caixas postais envolvidas poderão ser acessadas, vedada a divulgação de seus conteúdos.

3.17.2 A divulgação do conteúdo de mensagem que tenha sido acessada em função de manutenção técnica ou restauração de cópias de segurança será considerada violação de sigilo funcional.

3.18 A CGTI realizará o armazenamento de mensagens trafegadas e de outros dados do sistema de correio eletrônico, com os seguintes objetivos:

3.18.1 Integridade do sistema, por meio de cópias de segurança ("backup");

3.18.2 Recuperação de conteúdos de mensagens.

3.19 Os procedimentos técnicos que visem a apurar fatos envolvendo o sistema de correio eletrônico somente poderão ser realizados pela CGTI quando solicitados formalmente pela Corregedoria do Ibama ou em casos de cumprimento de ordem judicial.

3.20 A CGTI poderá implantar mecanismos de filtros de mensagens, com o objetivo de preservar a integridade do ambiente de rede do Ibama ou de seu sistema de correio eletrônico.

4 RESPONSABILIDADES

4.1 Compete à CGTI a disponibilização da infraestrutura computacional para a implementação do

serviço de correio eletrônico.

4.2 A solicitação de criação ou de exclusão de caixas postais do Ibama é de responsabilidade das chefias e dos ocupantes de cargo do Grupo de Direção e Assessoramento Superiores - DAS.

4.3 Compete à CGTI a manutenção do sistema e a gerência das caixas postais.

4.4 Compete à CGTI a designação da equipe de administradores do correio eletrônico de que trata esta Norma.

5 VEDAÇÕES

5.1 Para os fins desta Norma, são consideradas condutas de uso inadequado do sistema de correio eletrônico:

5.1.1 Acessar caixas postais de outros usuários, sem autorização prévia;

5.1.2 Incomodar qualquer usuário, seja por meio de quantidade, frequência, tamanho ou linguagem das mensagens, assunto ou destinação, de conteúdo inadequado ou que não estiver em conformidade com as atividades da instituição;

5.1.3 Insistir no envio de mensagens a qualquer pessoa que não as deseje receber;

5.1.4 Enviar mensagens que tenham como objetivo a promoção de produtos e serviços de caráter não institucional;

5.1.5 Reenviar ou propagar mensagens de "correntes" ou "pirâmides";

5.1.6 Fraudar quaisquer das informações do cabeçalho do remetente.

5.2 O descumprimento das disposições desta Norma ou o uso inadequado do sistema sujeitará o usuário à suspensão imediata do uso do correio eletrônico, como medida preventiva que vise a assegurar a integridade do sistema.

5.2.1 O restabelecimento do serviço somente ocorrerá mediante solicitação justificada da autoridade à qual esteja subordinado o servidor ou usuário especial, dirigida à CGTI.

5.2.2 Na hipótese de reincidência ou considerando-se a gravidade do fato, poderá ser caracterizada infração funcional, a ser apurada em processo administrativo disciplinar, sujeitando o infrator às penalidades previstas no art. 127 da Lei nº 8.112, de 11 de dezembro de 1990, sem prejuízo da responsabilidade penal e civil.

5.3 Os indícios de prática de procedimentos que possam ocasionar quebra de segurança ou violação das disposições constantes desta Norma devem ser comunicados à Equipe de Tratamento e Respostas em Incidentes de Rede do Ibama (Etir) para análise, avaliação, deliberação e adoção das providências cabíveis.

6 DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas a respeito desta Norma serão submetidos ao Comitê de Governança Digital - CGD e à Coordenação-geral de Tecnologia da Informação - CGTI.

7 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO III

Norma Complementar 06

Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma	REVISÃO	Emissão	FOLHA
06/NC/POSIC/CGD	01	20/09/2021	1
Gestão de Riscos de Segurança da Informação, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

ORIGEM

Comitê de Governança Digital do Ibama (CGD)

REFERÊNCIA NORMATIVA

- Instrução Normativa nº 3 GSI/PR, de 28 de maio de 2021
- ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão da Segurança da Informação;
- ABNT ISO/IEC 27002:2013 – Código de Prática para Controles de Segurança da Informação; ABNT NBR ISO/IEC 27005:2019 Gestão de riscos de segurança da informação; e
- Decreto nº 9.637/2018.

CAMPO DE APLICAÇÃO

Esta norma aplica-se no âmbito do Ibama.

Sumário

INFORMAÇÕES ADICIONAIS

Esta Norma Complementar substitui a NC 06/NC/POSIC/CSII, de 08/08/2014.

Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma	Revisão	Emissão	FOLHA
06/NC/POSIC/CGD	01	20/09/2021	2
Gestão de Riscos de Segurança da Informação, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

1 OBJETIVO

Estabelecer diretrizes e responsabilidades necessárias para a implantação do processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC no âmbito da no âmbito da Política de Segurança da Informação, Informática e Comunicações do Ibama - POSIC.

2 CONCEITOS E DEFINIÇÕES

Para o entendimento adequado desta Norma, em conformidade com a POSIC, considera-se:

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

2.2 Análise de riscos – uso sistemático de informações para identificar fontes e estimar o risco;

2.3 Análise/avaliação de riscos – processo completo de análise e avaliação de riscos;

2.4 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;

2.5 Avaliação de riscos – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

2.6 Comunicação do risco – troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;

2.7 Estimativa de riscos – processo utilizado para atribuir valores à probabilidade e consequências de um risco;

2.8 Evitar risco – uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

2.9 Gestão de Riscos de Segurança da Informação e Comunicações – conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

2.10 Identificação de riscos – processo para localizar, listar e caracterizar elementos do risco;

2.11 Reduzir risco – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

2.12 Reter risco – uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades, caso ocorra o risco identificado;

2.13 Riscos de Segurança da Informação e Comunicações – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

2.14 Transferir risco – forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

2.15 Tratamento dos riscos – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

2.16 Vulnerabilidade – conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

3 DIRETRIZES

3.1 O processo de Gestão de Riscos de Segurança da Informação e Comunicações deve estar alinhado ao planejamento estratégico da organização e também, política de gestão de riscos do Ibama.

3.2 A Gestão de Riscos de Segurança da Informação e Comunicações, objeto desta Norma Complementar, está limitada ao escopo das ações de Segurança da Informação e Comunicações e compreendem as medidas de proteção dos ativos de informação, conforme definido nesta Norma.

3.3 As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão, além de estarem alinhadas à respectiva Política de Segurança da Informação, Informática e Comunicações.

3.4 O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deve ser continuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações.

3.5 O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deve estar alinhado ao modelo denominado PDCA (Plan-Do-Check-Act), de modo a fomentar a sua melhoria continua.

3.6 A Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deverá produzir subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios.

3.7 O processo de gestão de riscos de segurança da informação tem por objetivo direcionar e controlar o risco de segurança da informação, a fim de adequá-lo aos níveis aceitáveis para o órgão ou entidade.

3.8. O processo de gestão de riscos de segurança da informação deverá fornecer à organização os seguintes documentos:

3.8.1 plano de gestão de riscos de segurança da informação;

3.8.2 relatório de identificação, análise e avaliação dos riscos de segurança da informação; e

3.8.3 relatório de tratamento de riscos de segurança da informação.

3.9 O plano de gestão de riscos de segurança da informação deverá conter, no mínimo:

3.9.1 a abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação e os ativos de informação que serão objeto de tratamento;

ANEXO IV
Norma Complementar 07

Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma	REVISÃO	Emissão	Folha
07/NC/POSIC/CGD	01	03/11/2021	1
Uso de Internet, Intranet e Extranet, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

ORIGEM

Comitê de Governança Digital do Ibama (CGD)

REFERÊNCIA NORMATIVA

- Lei n° 12965, de 23.04.2014 - Marco Civil da Internet;
- Lei n°12527, de 18.11.2011 – Lei de Acesso à Informação; Decreto nº 9.637, de 2018;
- Instrução Normativa 01 GSI/PR, de 27.05.2020;
- ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão da Segurança da Informação;
- ABNT ISO/IEC 27002:2013 – Código de Prática para Controles de Segurança da Informação; ABNT NBR ISO/IEC 27005:2019 - Gestão de riscos de segurança da informação.

CAMPO DE APLICAÇÃO

Esta norma aplica-se no âmbito do Ibama.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta Norma Complementar substitui a NC 07/NC/POSIC/CSII, de 08/08/2014.

	Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma		Revisão	Emissão	Folha
07/NC/POSIC/CGD		01	03/11/2021	2
Uso de Internet, Intranet e Extranet, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC				

1 OBJETIVO

Regulamentar procedimentos para o uso da Internet, Intranet e Extranet no Ibama, – em conformidade com a Política de Segurança da Informação, Informática e Comunicações - POSIC do Ibama.

2 CONCEITOS E DEFINIÇÕES

Para o entendimento adequado desta norma, em conformidade com a Posic, considera-se:

2.1 Equipe de Tratamento e Resposta a Incidentes e Riscos – ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

2.2 Extranet: rede de computadores da instituição com acesso aberto a clientes e parceiros;

2.3 Internet: rede mundial de computadores que permite a comunicação entre pessoas e organizações, independente da localização geográfica;

2.4 Intranet: rede privada, acessível apenas aos membros da organização que atende. Utiliza os mesmos recursos e protocolos da Internet, mas é comumente separada desta através de firewalls;;

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

2.6 Sítio (site): conjunto de informações e ou serviços disponíveis na Internet ou na Intranet, organizados em páginas eletrônicas e acessíveis por meio de endereços que identificam, de forma padronizada, sua origem e seu conteúdo;

2.7 Spam: e-mails não solicitados que geralmente são enviados para um grande número de pessoas;

2.8 Upload: envio de dados de um computador local para um computador ou servidor remoto;

2.9 VPN – acrônimo para Virtual Private Network (Rede Privada Virtual): refere-se a construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

3 DIRETRIZES

3.1 Os serviços de Internet, Intranet e Extranet disponibilizados ao usuário pela Instituição são uma concessão e não um direito, por isso devem ser utilizados somente como um canal

para pesquisas e busca de informações sobre assuntos de interesse estritamente profissionais;

3.2 A liberação do acesso para utilização da Internet, Intranet e Extranet será condicionada à concordância com os termos de responsabilidade, por meio dos quais o usuário declara ter conhecimento do disposto na Posic, nesta norma e nas demais normas vigentes.

3.3 O usuário deve utilizar os serviços de Internet, Intranet e Extranet observando a conformidade com a a legislação e o código de ética do Ibama.

3.4 Todo agente público (usuário) do Ibama que utilizar algum recurso computacional para acessar a Internet, a Intranet ou a Extranet, deverá obrigatoriamente possuir uma conta de acesso, denominada conta de usuário, a ser solicitada à Coordenação-geral de Tecnologia da Informação (CGTI) pela chefia imediata da unidade de lotação do usuário.

3.5 Nos computadores conectados à Intranet, todo usuário, para início da sessão de navegação, deverá ser autenticado mediante login no domínio da rede local.

3.6 Os computadores conectados à Intranet, e fora do domínio da rede local, serão bloqueados e seus usuários serão responsabilizados administrativamente.

3.7 O acesso à Internet, por meio da rede corporativa, deve ocorrer somente por equipamentos autorizados pela CGTI..

3.8 O acesso à Internet deve estar protegido por tecnologias de segurança, como antivirus, filtro de conteúdo e demais recursos para a proteção da rede, definidos em procedimentos de segurança específicos.

3.9 A CGTI poderá criar níveis diferenciados de acesso à Internet,de acordo com a necessidade de cada área ou coordenação.

3.10 Ao acessar um sítio não autorizado, o usuário será direcionado para uma página do Ibama contendo o motivo do bloqueio e a qual categoria a página bloqueada foi classificada.

3.11 O acesso à Internet é passível de monitoração e identificação.

3.12 Cabe à CGTI, desde que requerido formalmente, fornecer relatório de uso da Internet, por usuário.

3.13 Cabe à CGTI fornecer relatório de uso da Internet, contendo o resumo dos acessos aos sítios, por Unidade do Ibama, sempre que formalmente solicitado pelo Gabinete de Segurança Institucional da Presidência da República – GSI/PR ou pela Presidência do Ibama.

3.14 A CGTI poderá, quando houver falha de segurança ou comprometimento da estrutura de acesso à Internet, restringir ou proibir o acesso, a fim de garantir a continuidade e a normalidade dos serviços de rede.

3.15 A CGTI deverá manter o registro dos acessos à Internet realizados por meio da rede do Ibama pelo prazo de 01 (um) ano, contados a partir da data do acesso, conforme Art. 13º da Lei 12.965 da Presidência da República de 23/04/2014.

3.16 Após esse período, os LOGs de acesso deverão ser transferidos para fitas de backup e armazenadaos por 05 (cinco) anos.

3.17 Os procedimentos técnicos destinados a apurar irregularidades que envolvam o acesso à Internet, Intranet e Extranet deverão ser realizados pela CGTI e coordenados pelo Gestor de Segurança da Informação, desde que solicitados formalmente pela Polícia Federal ou

em caso de cumprimento de ordem judicial.

3.18 A definição das categorias, as regras de bloqueio a sítios e suas exceções serão definidas pela CGTI e divulgadas na Intranet/Extranet.

3.19 Os sítios relacionados às categorias abaixo serão bloqueados a todos os usuários do Ibama: :

3.19.1 Violência extrema (extreme);

3.19.2 Proxy anônimo (filter avoidance);

3.19.3 Jogos de azar (gambling);

3.19.4 Apologia ao ódio (hate speech);

3.19.5 Atividades ilegais (illegal activities);

3.19.6 Drogas (illegal drugs);

3.19.7 Pornografia (pornography).

3.20 O download e o upload de arquivos cujas extensões possam mascarar códigos maliciosos definidos pela CGTI serão bloqueados.

3.21 Arquivos que forem bloqueados por conter as extensões maliciosas, mas que são necessários para uso profissional e desenvolvimento do trabalho, poderão ser liberados mediante solicitação formal do responsável da unidade à CGTI, que analisará caso a caso.

3.22 É permitido aos usuários dos recursos computacionais do Ibama utilizar a Internet, Intranet e Extranet para:

3.22.1 Fins de complemento às atividades do setor;

3.22.2 Enriquecimento intelectual de seus servidores;

3.22.3 Como ferramenta para busca de informações que venham a contribuir para o desenvolvimento de suas atividades.

3.23 O acesso a recursos ou sítios com algum tipo de restrição poderá ser liberado mediante solicitação formal do responsável da unidade à CGTI.

3.24 O acesso a sítios que sobrecarreguem o tráfego de dados da rede do Ibama deverão ser controlados por meio de arquivos de logs. O uso excessivo e/ou acima do normal será comunicado aos usuários e a seus respectivos chefes por meio de relatórios.

3.25 Não é permitido aos usuários dos recursos computacionais do Ibama utilizar a Internet, Intranet e Extranet para:

3.25.1 Passar-se por outra pessoa ou dissimular sua identidade, sendo vedado o anonimato em qualquer situação;

3.25.2 Compartilhar logins e senhas mesmo que provisoriamente;

3.25.3 Invadir a privacidade de terceiros em busca de senhas e/ou dados privativos, violar sistemas de informação ou invadir VPNs;

3.25.4 Prejudicar intencionalmente outros usuários por meio de programas criados, alterados ou modificados para fins danosos ou para propagar códigos maliciosos – vírus, *keyloggers (registrador do teclado* em inglês) é um programa de computador do tipo *spyware* cuja finalidade é registrar tudo o que é digitado, quase sempre a fim de capturar senhas, números de cartão de crédito e afins)*, rootkits* (tipo de software, muitas das vezes

malicioso, projetado para esconder a existência de certos processos ou programas de métodos normais de detecção e permitir continuo acesso privilegiado a um computador)etc;

3.25.5 Realizar download ou upload de aplicativos de qualquer espécie para transportar códigos maliciosos, objetivando a instalação nos computadores dentro ou fora do ambiente do Ibama;

3.25.6 Inserir links ou hiperlinks nos sítios mantidos pelo Ibama, que redirecionam para páginas impróprias e/ou que violem a Posic;

3.25.7 Utilizar meios (dispositivos e ferramentas) que burlem as políticas de bloqueio aplicadas pelo Ibama.

3.25.8 Instalar, configurar ou manter equipamentos de informática, tais como modens e roteadores, na rede corporativa do Ibama sem prévia autorização da CGTI ou do NINFO.

3.25.9 Destruir ou corromper dados e informações armazenadas em servidores ou computadores de qualquer usuário;

3.25.10 Forjar endereços de máquinas (*MAC Address*), de rede (*Internet Protocol*) ou de correio eletrônico;

3.25.11 Efetuar o envio ou cópia de qualquer *software* licenciado e adquirido exclusivamente para o Ibama ou dados e informações de uso exclusivo e restrito da instituição;

3.25.12 Divulgar e/ou o compartilhar indevidamente, utilizando ferramentas de bate-papo ou transferência de arquivos, quaisquer informações sigilosas pela Internet, Intranet e Extranet.

4 RESPONSABILIDADES

4.1 Cabe à Presidência do Ibama, no âmbito de suas atribuições:

4.4.1 Aprovar as diretrizes gerais para acesso à Internet, Intranet e Extranet, observada, dentre outras, a respectiva Política de Segurança da Informação e Comunicações - POSIC;

4.1.2 Aprovar as categorias de acesso que deverão ser bloqueadas para todos os usuários;

4.1.3 Aprovar o plano de comunicação a ser utilizado quando houver falhas para este serviço;

4.1.4 Aprovar a aquisição de novas tecnologias que visem melhorar o acesso, o filtro, a segurança, a performance e a disponibilidade da Internet.

4.2 Cabe ao Comitê de Governança Digital (CGD), no âmbito de suas atribuições:

4.2.1 Sugerir modificações na norma de acesso à Internet, Intranet e Extranet;

4.2.2 Propor plano de implementação da respectiva norma.

4.3 Cabe à Coordenação-geral de Tecnologia da Informação (CGTI), no âmbito de suas atribuições:

4.3.1 Coordenar a implementação, implantação e manutenção da infraestrutura de acesso à Internet, Intranet e Extranet;

4.3.2 Elaborar o plano de comunicação quando houver problemas com este serviço;

4.3.3 Definir as categorias que deverão ser bloqueadas para todos os usuários

4.3.4 Definir os tipos de arquivos/extensões que deverão ser bloqueadas;

4.3.5 Prover relatórios, sob demanda, contendo as páginas mais acessadas, as páginas mais bloqueadas, a quantidade de vírus detectados e a utilização da largura de banda para a Internet, Intranet e Extranet;

4.3.6 Fomentar novas tecnologias que visem melhorar o acesso, o filtro, a segurança, a performance e a disponibilidade da Internet.

4.3.7 Sugerir novas tecnologias que visem melhorar o acesso, o filtro, a segurança, a performance e a disponibilidade da Internet;

4.3.8 Administrar os LOGs de acesso, incluindo o período de armazenamento em volumes e posterior migração para backups em fita.

4.4 Cabe aos Usuários, no âmbito de suas atribuições:

4.4.1 Garantir a segurança da informação que manipular, assim como dos recursos computacionais que fizer uso, observadas as disposições da Política de Segurança da Informação e Comunicações do Ibama.

4.4.2 Proteger a sua identidade eletrônica, senhas, credenciais de autenticação, autorizações ou quaisquer outros dispositivos de segurança, não podendo revelá-las a terceiros;

4.4.3 Responder pelo mau uso da conta e dos recursos computacionais em quaisquer circunstâncias;

4.4.4 Responder por atos de sua autoria que violem as regras de uso dos recursos computacionais, estando sujeito às penalidades definidas nesta Norma e na POSIC e, se for o caso, às penalidades impostas por outras instâncias;

4.4.5 Utilizar adequadamente a Internet, Intranet e Extranet disponibilizada pelo Ibama;

4.4.6 Reportar incidentes de segurança da informação à ETIR pelo e-mail etir.sede@ibama.gov.br;

4.4.7 Zelar pelo fiel cumprimento ao estabelecido nesta norma.

5 SANÇÕES E PENALIDADES

5.1 A utilização de sites e aplicativos no âmbito da rede internet e intranet não permitidos provocarão o imediato bloqueio do computador e notificação à chefia imediata para providências cabíveis. A liberação do computador ocorrerá após a identificação e a retirada dos sites e aplicativos do computador.

5.2 O usuário que realizar alguma das ações previstas no Art.23 desta norma, terá seus acessos à Internet e à Rede do Ibama imediatamente bloqueados e sua chefia imediata será notificada para providências cabíveis. A liberação do computador ocorrerá após averiguação dos fatos. A ETIR será comunicada do incidente por meio de um relatório detalhado, contendo o número de patrimônio do equipamento, o nome do usuário principal, o horário em que ocorreu o incidente e os efeitos que porventura tenha causado na intranet e na extranet.

5.3 O não cumprimento desta norma sujeita o usuário às penalidades previstas na Política de Segurança de Informação e Comunicações – POSIC do Ibama.

6 DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas a respeito desta norma serão submetidos ao Comitê de Governança Digital - CGD e à Coordenação-geral de Tecnologia da Informação - CGTI.

7 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO V
Norma Complementar 08

Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma	Revisão	Emissão	Folha
08/NC/POSIC/CGD	01	20/09/2021	1
Classificação de Documentos Sigilosos, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

ORIGEM

Comitê de Governança Digital do Ibama (CGD)

REFERÊNCIA NORMATIVA

- Lei 12.527/2011;
- Decreto 7.724/2012;
- Decreto 7.845/2012;
- Portaria Ibama 2421/2017

CAMPO DE APLICAÇÃO

Esta norma aplica-se no âmbito do Ibama

SUMÁRIO

INFORMAÇÕES ADICIONAIS

No Brasil, o acesso à informação encontra-se consolidado como direito fundamental previsto no inciso XXXIII, do art. 5º da Constituição Federal de 1988 (CF/88), que assim dispõe:

> *"XXXIII - Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado."*

A Lei de Acesso à Informação – LAI, garante ao cidadão o acesso às informações produzidas ou custodiadas pela Administração Pública, estabelecendo procedimentos que visam garantir que estas informações estejam disponíveis de maneira ampla à sociedade. Por

princípio, a divulgação é a regra e o sigilo, a exceção. Portanto, na excepcionalidade, a LAI vem proteger as informações que, em situações especiais, não poderão ser divulgadas ou não poderão estar acessíveis por prazos estabelecidos.

Esta Norma Complementar substitui a NC 08/NC/POSIC/CSII, de 08/08/2014.

Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma	Revisão	Emissão	Folha
08/NC/POSIC/CGD	01	20/09/2021	2
Classificação de Documentos Sigilosos, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

1 OBJETIVO

Regulamentar procedimentos referentes à produção, expedição, recebimento, tramitação e credenciamento de documentos sigilosos no Ibama, no âmbito da Política de Segurança da Informação, Informática e Comunicações do Ibama - POSIC.

2 CONCEITOS E DEFINIÇÕES

2.1 A concepção de "informação sigilosa" e "informação classificada em grau de sigilo", apesar dos termos estarem em oposição à informação ostensiva, ou seja, aquela acessível ao cidadão, se divergem na aplicação:

2.1.1 Informação Sigilosa, é a que por algum motivo previsto em lei, deverá ter seu acesso restrito.

2.1.2 Informação Classificada em Grau de Sigilo, refere-se a um tipo específico de informação sigilosa que tem sua restrição amparada pelos Arts. 23 e 24 da Lei de Acesso à Informação – LAI e pelo Art. 20 do Decreto 7.724/2012.

2.2 Toda informação classificada em grau de sigilo é, também, sigilosa, porém nem toda informação sigilosa será classificada em grau de sigilo, uma vez que esta contém informações com acesso restringido em virtude de uma legislação específica.

2.3 Para o entendimento adequado desta norma, em conformidade com a Posic, considera-se:

2.3.1 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 (APF);

2.3.2 Autenticidade – qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

2.3.3 Ciclo de vida da informação – ciclo formado pelas fases da produção e recepção, organização, uso, disseminação e destinação;

2.3.4 Classificação da informação – atribuição de grau de sigilo às informações nos termos da Lei nº 12.527/2011, Lei de Acesso à Informação (LAI);

2.3.5 Código de Indexação de Documento que contém Informação Classificada (CIDIC) –

código alfanumérico que indexa documento com informação classificada em qualquer grau de sigilo, a primeira parte do CIDIC deve prever número de posições que atendam ao Número Único de Protocolo-NUP, que é um código composto por 17 dígitos numéricos. A segunda parte do CIDIC, separada da primeira parte por um ponto (.), iniciará sempre por um caractere alfabético "S" para Secreto ou "R" para Reservado) e deverá prever até o máximo de 28 dígitos, com caracteres alfanuméricos e separadores. Os separadores utilizados serão os sinais gráficos: ponto (.) para os campos e barra (/) para as datas.

- NUP: número único de protocolo – deve ser preenchido por 17 dígitos;
- Grau de Sigilo: será preenchido com as iniciais S – Secreto ou R – Reservado;
- Código do Assunto: correspondente Art. 52, parágrafo II, anexo II do Decreto 7.845;
- Data de Produção: criação do documento;
- Data de Desclassificação: data em que a informação perderá o prazo de sigilo;
- Indicação da Reclassificação: S se houver prorrogação do prazo (somente para o grau ultrassecreto) e N se não houver (para os graus Secreto e Reservado, caso do Ibama)
- Data da Prorrogação: não se aplica ao Ibama.

Ex. : 02001.002537/2013-99.S.12.10/11/2013.10/11/2028.N

2.3.6 Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) – comissão interna que, nos termos do art. 34 do Decreto nº 7.724/2012, tem a atribuição de assessorar, opinar, propor e subsidiar a autoridade classificadora. No Ibama, foi instituída pela Portaria nº 2381, de 08 de outubro de 2020;

2.3.7 Confidencialidade – garantia de que a informação é acessível somente por usuários autorizados;

2.3.8 Dados processados – dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

2.3.9 Desclassificação – cancelamento da classificação atual de uma informação pela autoridade competente ou por transcurso de prazo;

2.3.10 Disponibilidade – qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

2.3.11 Documento – unidade de registro de informações, qualquer que seja o suporte ou formato;

2.3.12 Documento preparatório – documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas;

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

2.3.14 Informação categorizada como sigilosa – Informação que foi marcada como sigilosa no Sistema Eletrônico de Informação – SEI;

2.3.15 Informação ostensiva – em oposição à informação sigilosa, é qualquer informação não submetida à restrição de acesso público;

2.3.16 Informação pessoal – informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

2.3.17 Informação restrita – informações classificadas como sigilosas (reservada, secreta

ou ultrassecreta) ou consideradas de acesso restrito nos termos da Lei de Acesso à Informação ou protegidas pelas demais hipóteses legais de sigilo e restrição;

2.3.18 informação sigilosa - aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

2.3.19 Integridade – qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

2.3.20 Tratamento da informação - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

2.3.21 Reclassificação – alteração da classificação da informação pela autoridade classificadora;

2.3.22 Termo de Classificação de Informação (TCI) – formulário que formaliza a decisão de classificação, desclassificação, reclassificação ou alteração do prazo de sigilo de informação classificada em qualquer grau.

3 DIRETRIZES

3.1 A classificação dos documentos/processos externos e internos no Ibama seguirão as diretrizes prescritas na Lei 12.527, de 18 de novembro de 2011 e nos seus Decretos reguladores 7.724, de 16 de maio de 2012 e 7.845,de 14 de novembro de 2012, bem como na Portaria Ibama n° 2.421, de 14 de novembro de 2017.

3.2 As informação institucional do Ibama, em quaisquer suporte, materiais, áreas, comunicações e sistemas de informação institucionais, é patrimônio do Estado Brasileiro e deve ser tratada segundo os preceitos descritos nesta Norma Complementar e nos termos da legislação pertinente em vigor.

3.3 O Ibama poderá classificar como sigilosos documentos/processos externos que não tenham tal identificação, de acordo com a legislação, a necessidade e o assunto, para efeitos de segurança da informação.

3.3.1 Os documentos/processos externos que derem entrada no Ibama como sigilosos não terão sua classificação alterada, salvo se a instituição de origem assim o requerer oficialmente.

3.4 Para os documentos definidos como sigilosos, deverá ser elaborado o Termo de Classificação de Informação – TCI (Anexo I), onde será registrado, dentre outros dados, o grau de sigilo, a categoria na qual se enquadra a informação exclusivamente classificada pela LAI, o tipo de documento, as razões da classificação, o prazo de sigilo ou evento que definirá o seu término, o fundamento da classificação e a identificação da autoridade classificadora.

3.4.1 O TCI acompanhará o documento principal e deverá conter o histórico dos eventos relativos à ratificação, à desclassificação e à reavaliação do grau de sigilo da informação.

3.4.2 Nos casos em que um documento contiver informações a serem classificadas em diferentes graus de sigilo, deverão ser observados o procedimento e a competência para o grau de sigilo mais elevado.

3.4.3 As partes do documento não classificadas, deve-se garantir o acesso por meio de certidão, extrato ou cópia, prezando-se pela ocultação da parte sob sigilo.

3.4.4 Não se deve preencher TCI para aquelas informações cujo sigilo esteja previsto em outras legislações (como bancária, fiscal e tributária), documentos preparatórios e informações pessoais.

3.5 Para a informação classificada como secreta deverá ser produzido TCI a ser encaminhado ao Presidente do Ibama para assinatura, realizando o trâmite de acordo com as instruções estabelecidas pelo Art. 26 do Decreto 7.845 de 2012.

3.6 A classificação de informações no grau Reservado, será de competência dos ocupantes dos seguintes cargos de direção:

3.6.1 Chefes da Divisão Técnico Ambiental, nas Superintendências Estaduais do Ibama

3.6.2 Assessores das diretorias

3.6.3 Coordenador da Coordenação de Inteligência de Fiscalização da Diretoria de Proteção Ambiental.

3.6.3.1 É vedada a subdelegação da competência de que trata este item.

3.6.3.2 Para informações no grau Reservado, o TCI deverá ser produzido e ratificado apenas para controle do prazo de desclassificação.

3.7 A decisão de desclassificação, reclassificação ou alteração de prazo de sigilo deve ser formalizada em TCI, devidamente motivada e com assinatura da autoridade competente.

3.8 A tramitação e expedição de documentos e processos classificados ou restritos deverão observar o disposto no Art. 26 do Decreto 7.845/12, sendo os seguintes procedimentos:

3.8.1 serão acondicionados em envelopes duplos, sendo o externo livre de qualquer indicação do grau de sigilo ou do teor do documento ou processo;

3.8.2 no envelope interno serão apostos o destinatário e o grau de sigilo do documento/processo, de modo a serem identificados logo que removido o envelope externo;

3.8.3 o envelope interno será fechado, lacrado e expedido mediante recibo, que indicará, necessariamente, remetente, destinatário e número ou outro indicativo que identifique o documento/processo;

3.8.4 sempre que o assunto for considerado de interesse exclusivo do destinatário, será inscrita a palavra "pessoal" no envelope que contém o documento/processo.

3.9 Na tramitação de um documento com informação classificada, seja por expediente ou correspondência, a unidade responsável pelo atendimento (protocolo) deverá cumprir os procedimentos a seguir:

3.9.1 verificar a integridade do meio de recebimento e conferir os dados do destinatário;

3.9.2 abrir o envelope externo, conferir os dados do remetente no envelope interno, bem como a identificação de "documento sigiloso";

3.9.3 providenciar a entrega, em mãos, ao destinatário citado no envelope, com registro de entrega; e

3.9.4 observado o indício de violação ou de irregularidade, o responsável pelo atendimento deve registrar o fato e comunicar o chefe imediato e o destinatário, que

deverão informar imediatamente ao remetente.

3.9.5 O destinatário, ao receber a informação, deverá informar ao remetente o recebimento do expediente, no prazo mais curto possível.

3.10 O documento com informação classificada em grau de sigilo, de acordo com a Lei nº 12.527/2011, deve possuir forma híbrida e ter apenas sua tramitação registrada no SEI, enquanto os documentos devem constar apenas no processo físico, sem a captura para o sistema eletrônico.

3.11 A unidade administrativa detentora do processo eletrônico sigiloso, deverá de ofício, segundo legislação aplicável, definir ou redefinir o nível de acesso sempre que necessário, ampliando ou limitando seu acesso, especialmente quando não mais subsistir a situação de fato ou de direito que justifique a atribuição de nível de acesso limitado.

3.12 Os procedimentos relativos à disponibilização, à classificação, ao tratamento e a gestão da informação de natureza restrita, no âmbito do Ibama, obedecerão às disposições contidas em legislação específica, em observância aos princípios e diretrizes estabelecidas pela POSIC.

3.13 Documentos e processos que se enquadrem nas hipóteses de classificação da informação previstas nos Arts. 23 e24 da LAI, não devem ser produzidos ou inseridos nos sistemas informatizados de gestão de documentos e processos do Ibama.

3.13.1 Ressalvando que, o SEI é importante no apoio à classificação da informação, por ser o sistema onde será feito o registro dos documentos classificados sob a geração do Número Único de Protocolo (NUP) e da composição do Código de Indexação de Documento que Contém Informação Classificada (CIDIC).

3.14 A informação que deva ser classificada em grau de sigilo, em momento posterior à sua produção ou inserção no SEI. Para esses casos, é necessário cumprir os seguintes procedimentos:

3.14.1 Alterar, no processo eletrônico, o nível de acesso para a categoria “Sigiloso”, definindo seu embasamento conforme a lei, por meio do rol de Hipóteses Legais disponibilizada no SEI.

3.14.2 Seguir o fluxo definido para criar documento classificado. Como a regra é prezar pela transparência da informação, qualquer restrição a ser adotada deverá ser justificada.

3.15 É vedada a cópia de documentos sigilosos.

3.16 O Ibama deverá divulgar anualmente, o Rol ou lista das informações classificadas e desclassificadas em grau de sigilo em seus sítios na internet, conforme estabelece o art. 45 do Decreto Nº 7.724/2012.

3.16.1 As informações cujo sigilo se deva a outras legislações (como bancária, fiscal e tributária), documentos preparatórios e informações pessoais não devem ser inseridas nesse rol.

3.16.2 A autoridade máxima de cada unidade, na sede e nos Estados, de acordo com o previsto no Art. 9º da Portaria Ibama n° 2.421/2017, deverá encaminhar o rol das informações classificadas e desclassificadas (Anexos II e III), à Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS), até o dia 1º de maio de cada ano, para que sejam compilados em um único rol e posterior chancela da presidência e publicação no sítio institucional conforme determinado pelo Art. 45 do Decreto 7.724 de 16 de maio de 2012.

4 RESPONSABILIDADES

4.1 É de responsabilidade de cada unidade do Ibama, detentora de informação sigilosa, a guarda dos documentos/processos em trâmite.

4.2 A delegação de competência para classificar a informação sigilosas está previsto na Portaria nº 2.421/17 do Ibama.

4.3 A Portaria n° 2.421, de 14 de novembro de 2017, instituiu a Comissão Permanente de Avaliação de Documentos Sigilosos do Ibama (CPADS) tendo as seguintes atribuições:

4.3.1 opinar sobre a informação produzida no âmbito de sua atuação para fins de classificação em qualquer grau de sigilo;

4.3.2 assessorar a autoridade classificadora ou a autoridade hierarquicamente superior quanto à desclassificação, reclassificação ou reavaliação de informação classificada em qualquer grau de sigilo;

4.3.3 propor o destino das informações desclassificadas, indicando os documentos para guarda permanente, observado o disposto na Lei nº 8.159, de 8 de janeiro de 1991; e

4.3.4 subsidiar a elaboração do rol anual de informações desclassificadas e documentos classificados em cada grau de sigilo, a ser disponibilizado na Internet.

4.5 A legislação vigente prevê que o agente público poderá ser responsabilizado nos casos em que obstruir acesso à informação ostensiva e nos que divulgar informação sigilosa.

5 DISPOSIÇÕES GERAIS

5.1 As dúvidas a respeito desta Norma serão submetidas ao Comitê de Governança Digital - CGD e à Comissão Permanente de Avaliação de Documentos Sigilosos do Ibama - CPADS, os casos omissos serão resolvidos pela Presidência do Ibama.

5.2 O uso inadequado do SEI-Ibama e a divulgação de informações pessoais, bem como de dados considerados sensíveis e sigilosos de acordo com a legislação vigente, ficam sujeitos à apuração de responsabilidade, na forma da legislação em vigor.

6 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO I

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO
ÓRGÃO/ENTIDADE:

CÓDIGO DE INDEXAÇÃO:	
GRAU DE SIGILO:	
CATEGORIA:	
TIPO DE DOCUMENTO:	
DATA DE PRODUÇÃO:	
FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO:	
RAZÕES PARA A CLASSIFICAÇÃO: (idêntico ao grau de sigilo do documento)	
PRAZO DA RESTRIÇÃO DE ACESSO:	
DATA DE CLASSIFICAÇÃO:	
AUTORIDADE CLASSIFICADORA	Nome:
	Cargo:
AUTORIDADE RATIFICADORA (quando aplicável)	Nome:
	Cargo:
DESCLASSIFICAÇÃO em__/____/_____ (quando aplicável)	Nome:
	Cargo:
RECLASSIFICAÇÃO em__/____/_____ (quando aplicável)	Nome:
	Cargo:
REDUÇÃO DE PRAZO em__/____/_____ (quando aplicável)	Nome:
	Cargo:
PRORROGAÇÃO DE PRAZO em_/_____/_____ (quando aplicável)	Nome:
	Cargo:
ASSINATURA DA AUTORIDADE CLASSIFICADORA	
ASSINATURA DA AUTORIDADE RATIFICADORA (quando aplicável) _____ ASSINATURA DA AUTORIDADE responsável por DESCLASSIFICAÇÃO (quando aplicável) _____ ASSINATURA DA AUTORIDADE responsável por RECLASSIFICAÇÃO (quando aplicável) _____ ASSINATURA DA AUTORIDADE responsável por REDUÇÃO DE PRAZO (quando aplicável) _____ ASSINATURA DA AUTORIDADE responsável por PRORROGAÇÃO DE PRAZO (quando aplicável)	

ANEXO II

INFORMAÇÕES CLASSIFICADAS

TIC – 2017/2018								
Nº Ord	CIDIC	Catego-ria	Dispositivo Legal	Data de Produ-ção	Data de Classifica-ção	Data de Des-classificação	Prazo da Classifica-ção	Assunto

1	02001.000004/2016-89.R.12.21/06/2016.21/06/2021.N	12 – Meio Ambiente	-Art. 23, Inciso VIII daLei n 12.527/2011;- Art. 25, Inciso IX doDec. 7.724/2012;- Portaria Normativa –Ibama n° 29 e 30, de28 de novembro de 2013.	21/06/2016	21/06/2016	21/06/2021	5 anos	Venda de Sentenças

ANEXO III

INFORMAÇÕES DESCLASSIFICADAS

Informações Desclassificadas 2017/2018						
Nº Ord	**Número Único de Protocolo – NUP**	**Grau de Sigilo**	**Data de produção**	**Data de desclassificação**	**Razões da Classificação**	**Assunto**
1	02022.000195/2013-11	Secreto	02/03/2013	02/03/2028	A publicação poderá comprometer as atividades de fiscalização	Processo de pesquisa de remessade amostra de patrimônio genético da flora silvestre

ANEXO VI
Norma Complementar 09

Ministério do Meio Ambiente **Instituto do Meio Ambiente e dos Recursos Naturais Renováveis**			
Número da Norma	Revisão	Emissão	Folha
09/NC/POSIC/CGD	01	20/09/2021	1
Uso de auditórios e salas do Ibama para o serviço de videoconferência, no âmbito da Política de Segurança da Informação, Informática e Comunicações -POSIC			

ORIGEM

Comitê de Governança Digital do Ibama (CGD)

REFERÊNCIA NORMATIVA

- Decreto nº 9.637, de 2018 e
- Política de Segurança da Informação, Informática e Comunicações – POSIC/Ibama.

CAMPO DE APLICAÇÃO

Esta norma aplica-se aos servidores e colaboradores do Ibama.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta Norma Complementar substitui a NC 09/NC/POSIC/CSII, de 01/09/2014.

IBAMA MMA	Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma		Revisão	Emissão	Folha
09/NC/POSIC/CGD		01	20/09/2021	2
Uso de auditórios e salas do Ibama para o serviço de videoconferência, no âmbito da Política de Segurança da Informação, Informática e Comunicações -POSIC				

1 CONSIDERAÇÕES INICIAIS

O serviço de videoconferência dinamiza eficazmente a comunicação entre os dirigentes e funcionários do Ibama pois dispensa o deslocamento dos participantes de reuniões, treinamentos e outros eventos e assim economiza diárias e passagens para servidores e colaboradores eventuais.

2 OBJETIVO

Estabelecer diretrizes e responsabilidades necessárias para os procedimento de uso do serviço de videoconferência no âmbito da Plítica de Serguranã da Informação, Informática e Comunicações – POSIC do Ibama.

3 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma complementar, entende-se por:

3.1 Videoconferência: serviço de comunicação capaz de promover interatividade entre as pessoas que estão em locais geograficamente distintos, com comunicação audiovisual em tempo real;

3.2 Videoconferência: Serviço de comunicação capaz de promover interatividade entre pessoas que estão em locais geograricamente distintos, com comunicação audiovisual em tempo real;

3.3 Sistema de videoconferência: O conjunto de equipamentos, aparelhos, acessórios de áudio, vídeo e dados que, interligados entre si, constituem o recurso tecnológico para realização da videoconferência; e

3.4 Site: local remoto provido de um sistema de videoconferência que permite conexão com outros sistemas.

4 DIRETRIZES

4.1 As sessões de videoconferência iniciarão preferencialmente de segunda a sexta-feira a partir das 9h (nove horas), para possibilitar testes prévios de configuração e conexão.

4.2 Toda atividade de videoconferência deve ser comprovadamente associada às atividades do Instituto.

4.3 Justifica-se o uso da videoconferência quando as atividades a serem desenvolvidas necessitem de um meio de comunicação rápido, no qual sejam utilizados os recursos da solução e que elimine ou reduza despesas dos participantes com passagens, diárias e outros.

4.4 O usuário interessado em usar o serviço de videoconferência deverá preencher de modo claro e objetivo todos os campos obrigatórios do formulário "Solicitação de Uso da Videoconferência" disponível no SEI.

4.4.1 O formulário mencionado no caput deverá ser encaminhado à Assessoria de Comunicação – ASCOM juntamente com o formulário "Reserva de auditório", que deverá ser encaminhado ao Serviço de Manutenção Predial – SEPRED, para reserva do espaço, com antecedência mínima de sete dias úteis da data do evento.

4.4.2 A ASCOM terá o prazo de dois dias úteis para avaliar a solicitação e, em caso de deferimento, encaminhar o formulário à Coordenação- Geral de Tecnologia da Informação – CGTI para conhecimento e providências.

4.4.3 O não preenchimento dos campos obrigatórios do formulário poderá impedir a realização da sessão de videoconferência e, consequentemente, ensejar o cancelamento do evento.

4.4.4 Para participar de uma sessão de videoconferência, o solicitante deverá concordar com esta norma, submetendo eventuais dúvidas à equipe técnica, por meio de despacho no SEI à CGTI antes do evento.

4.5 O sistema de videoconferência oferecerá os seguintes serviços:

4.5.1 Videoconferência com conexões por meio da Internet (IP);

4.5.2 Gravação da videoconferência em mídias (CD, DVD, pendrive, etc); e

4.5.3 Disponibilização do sinal de áudio e vídeo em tempo real através da internet (streaming), durante o evento.

4.6 O interessado em gravar a videoconferência deverá entregar as mídias ao CGTI antes do início do evento e buscá-las ao final.

4.7 Se houver necessidade de tradução simultânea, a equipe ou empresa prestadora desse serviço deverá ser contratada diretamente pelo interessado, que deverá assumir todos os custos da prestação do serviço e dos equipamentos necessários para tal.

4.7.1 A equipe ou empresa a ser contratada deverá, antes de firmar qualquer contrato com o interessado, conhecer o sistema de videoconferência do Ibama, inteirar-se das normas de segurança pertinentes e analisar os equipamentos, aparelhos e pessoal existentes e a compatibilidade entre os equipamentos, testá-los com antecedência mínima de quinze dias úteis da data do evento e providenciar os recursos humanos adicionais para execução do evento.

4.7.2 Poderão ser reconfigurados os equipamentos de áudio, vídeo e afins, desde que não comprometa o funcionamento do sistema para outros eventos, e observado o disposto 4.15 da presente norma.

4.8 O sinal de áudio e vídeo poderá ser disponibilizado em tempo real pela internet (streaming) durante o evento. Tal serviço será providenciado pela equipe técnica da CGTI.

4.8.1 A solicitação desse serviço também deverá constar no formulário da Videoconferência" mencionado pelo item 4.4, para que a equipe técnica do Ibama solicite a reserva do servidor de streaming à CGTI.

4.9 Os testes de conexões com outros sites que participarão do evento deverão ser feitos diretamente pela equipe técnica da videoconferência, com antecedência mínima de 45 minutos da hora agendada para início do evento, facultado ao solicitante participar dos testes.

4.10 Quando for preciso apresentar conteúdos eletrônicos em mídias diversas durante a videoconferência, os conteúdos deverão ser disponibilizados para a CGTI com antecedência mínima de três dias úteis do início do evento para os devidos testes.

4.10.1 Os conteúdos deverão assegurar perfeitas condições de leitura aos participantes remotos em seus respectivos equipamentos.

4.11 A procura de salas de videoconferências em outras empresas, instituições e outros locais (sítio remoto), bem como contatos e agendamento de data e horário com os participantes remotos do evento cujo sistema será conectado ao do Ibama, serão de inteira responsabilidade do interessado na sessão de videoconferência.

4.11.1 Após identificada a sala, a equipe técnica responsável do sítio remoto deverá manter contatos com a equipe técnica do Ibama para realização dos testes e demais providências necessárias para realizar o evento.

4.12 A comunicação em língua estrangeira durante a preparação e a realização de videoconferência é de responsabilidade do solicitante.

4.13 As solicitações de videoconferência serão atendidas:

4.13.1 Conforme a ordem de recebimento da "Solicitação de Uso da Videoconferência" pela ASCOM; e

4.13.2 Mediante a disponibilidade dos locais, bem como da equipe técnica para a data e horário do evento pretendido.

4.13.3 Os casos excepcionais serão analisados e atendidos conforme a disponibilidade de recursos e de pessoal.

4.14 O cancelamento de eventos agendados deverá ocorrer pelo processo de solicitação, por despacho ao SEPRED e à ASCOM e com no mínimo três dias de antecedência ao evento.

4.15 O Ibama não fará nenhuma adaptação, alteração ou reconfiguração complexa – como,

por exemplo, corte de cabos ou substituição de conectores – para equipamentos de videoconferência incompativeis, exceto as reconfigurações técnicas gerais permitidas pelo sistema e que podem ser ativadas através dos controles existentes.

4.16 Quanto ao uso da sala:

4.16.1 É proibido consumir alimentos na sala de videoconferência;

4.16.2 Danos causados aos equipamentos e aparelhos por mau uso implicarão o ressarcimento ao Ibama para reparo ou reposição do bem danificado; e

4.16.3 Telefones celulares devem ser mantidos desligados ou no modo silencioso durante a videoconferência.

5 RESPONSABILIDADES

5.1 A operação do sistema de videoconferência na sede do Ibama é de responsabilidade da equipe técnica formada pela CGTI com apoio da Ascom e do Núcleo de Informática (NINFO) das superintendências estaduais do Ibama.

5.2 Os equipamentos deverão ser operados somente por técnicos devidamente treinados, capacitados e autorizados para tal.

5.3 Todos os agentes públicos do Ibama deverão conhecer esta norma complementar e a Política de Segurança da Informação, Informática e Comunicações do Instituto, bem como cumprir todos os procedimentos sob o aspecto de responsabilidade pelo zelo da sala de videoconferência (móveis, aparelhos, equipamentos).

5.4 Toda sessão de videoconferência deverá ser acompanhada no local por, pelo menos, um técnico do Ibama devidamente treinado e capacitado para tal.

5.5 Compete à equipe técnica que desempenha atividades junto à sala de videoconferência:

5.5.1 Zelar pelos equipamentos, aparelhos e toda infraestrutura da sala em permanente condição de uso, devendo, sempre que necessário, tomar as providências cabíveis sob o aspecto de manutenção preventiva, corretiva, reconfiguração de equipamentos ou aparelhos, limpeza, organização da sala e outros;

5.5.2 Abrir a sala de videoconferência, ligar todos equipamentos e aparelhos, testá-los, reconfigurá- los quando necessário, e preparar toda infraestrutura necessária para a sessão de videoconferência com antecedência mínima de 45 minutos ao início do evento; e

5.5.3 Ao final do evento, desligar todos equipamentos e aparelhos, sistema de climatização, de iluminação e de ventilação e fechar todas as portas da sala.

5.6 Compete à equipe técnica e ao responsável pelo evento acompanhar e orientar os participantes dos eventos quanto às condições de uso da sala.

5.7 O organizador do evento deverá respeitar o limite de capacidade de participantes do ambiente onde será realizada a videoconferência.

5.8. Compete ao apresentador:

5.8.1 Comparecer à sala de videoconferência do Ibama com antecedência mínima de 30 minutos do início do evento;

5.8.2 Testar as mídias a serem apresentadas com três dias úteis de antecedência, tanto em outro micro, como no notebook da sala de videoconferência;

e

5.8.3 Desligar o microfone quando estiver apenas ouvindo o locutor remoto, para evitar ruídos aos participantes remotos.

5.9 Compete aos participantes comparecer à sala de videoconferência com antecedência mínima de quinze minutos.

6 DISPOSIÇÕES GERAIS

6.1 Em caso de violação das regras gerais estabelecidas nesta norma, serão aplicadas as penalidades previstas na Política de Segurança da Informação, Informática e Comunicações do Ibama.

6.2 Apenas servidores do Quadro Permanente do Ibama e ocupantes de cargo D.A.S, no desenvolvimento de trabalhos de interesse do Instituto, podem solicitar o serviço.

6.3 Os casos omissos e as dúvidas a respeito desta norma serão submetidos ao Comitê de Governança Digital - CGD e à Coordenação-geral de Tecnologia da Informação - CGTI.

7 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação

ANEXO VII

Norma Complementar 10

Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma	Revisão	Emissão	Folha
10/NC/POSIC/CGD	01	20/09/2021	1
NC 10 - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, no âmbito da Política de Segurança da Informação, Informática eComunicações - POSIC			

ORIGEM

Comitê de Governança Digital do Ibama (CGD)

REFERÊNCIA NORMATIVA

- Decreto nº 9.637, de 2018;
- Instrução Normativa 01 GSI/PR, de 13 de junho de 2008;
- Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009; Norma Complementar nº 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010;

- ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão da Segurança da Informação;
- ABNT ISO/IEC 27002:2013 – Código de Prática para Controles de Segurança da Informação; ISO/IEC 27035 - 1:2016 – Information Security Incident Management; e
- Portaria Normativa Ibama nº 14, de 13.05.2016 - Instituição e funcionamento da ETIR.

CAMPO DE APLICAÇÃO

Esta norma aplica-se no âmbito do Ibama.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta Norma Complementar substitui a NC 10/NC/POSIC/CSII, de 17/04/2015.

1 OBJETIVO

Estabelecer diretrizes e responsabilidades necessárias para implantar a Equipe de Tratamento

e Resposta a Incidentes em Redes Computacionais – ETIR – no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC do Ibama.

2 CONCEITOS E DEFINIÇÕES

Para o entendimento adequado desta norma, em conformidade com a POSIC, considera-se:

2.1 Agente Responsável – servidor público ocupante de cargo efetivo do Instituto incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR;

2.2 Ameaça – conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou ativo;

2.3 Artefato malicioso – programa de computador, ou fragmento de programa, construído para provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou redes computacionais;

2.4 Ataque – ação que constitui uma tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não integro, ou indisponível;

2.5 Ataque de negação de serviço – ataque que consiste em impedir o acesso autorizado a um recurso ou atrasar operações ou funções valiosas;

2.6 Ativo – algo que tenha valor para o Instituto (informação, serviços, reputação, imagem etc);

2.7 CAIS/RNP – Centro de Atendimento a Incidentes de Segurança, da Rede Nacional de Ensino e Pesquisa. Atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes;

2.8 Cert.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira;

2.9 Central de atendimento Atende TI – ponto central de contato entre os usuários do Ibama e o departamento de tecnologia da informação. Responsável por abrir, encaminhar, escalonar, monitorar e fechar os incidentes computacionais no Ibama;

2.10 Comunidade ou público-alvo – conjunto de pessoas, setores, órgãos ou entidades atendidas pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR;

2.11 Cross-site scripting ou XSS – categoria das vulnerabilidades de segurança de computadores que deixam um site suscetivel a fornecer a um usuário, sem autorização, um script de cliente (client-side script) enviado por outro usuário através das entradas do site. Usuários mal intencionados podem usar tais vulnerabilidades para violar controles de acesso. Elas podem ser combatidas através da validação das entradas de usuário;

2.12 CTIR Gov – Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. Está subordinado ao Departamento de Segurança de Informação (DSI), do Gabinete de Segurança Institucional da Presidência da República (GSI/PR);

2.13 Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR –

equipe responsável por receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança em redes computacionais;

2.14 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 falha de controles, ou situação previamente desconhecida que possa ser relevante para a segurança da informação;

2.15 Incidente comum – incidente cuja criticidade se classifica como “muito baixa”, “baixa” ou “média”;

2.16 Incidente crítico – incidente cuja criticidade se classifica como “crítica” ou “alta”;

2.17 Incidente de segurança - um ou uma série de eventos indesejados ou inesperados de segurança da informação que tem probabilidade significativa de comprometer operações de negócio e ameaçar a segurança da informação;

2.18 Serviço - conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR;

2.19 Spamdexing - manipulação intencional e não-autorizada de índice de motor de busca;

2.20 Tratamento de incidentes de segurança em redes computacionais - serviço de recepção, filtro, classificação e resposta às solicitações e alertas e análise dos incidentes de segurança, procurando extrair informações para interromper a ação maliciosa e também identificar tendências;

2.21 Vulnerabilidade - conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, o qual pode ser mitigado por uma ação interna de segurança da informação.

3DIRETRIZES

3.1 A Gestão de Tratamento e Resposta a Incidentes em Redes Computacionais – GETIR no Ibama será criada e mantida pela ETIR com apoio do Comitê de Governança Digital - CGD.

3.2 O Gestor de Segurança da Informação e Comunicações do Ibama será o responsável por coordenar o treinamento e o aperfeiçoamento técnico da ETIR e solicitar os recursos materiais e tecnológicos necessários à execução das suas atividades.

3.3 O Agente Responsável será o responsável pela ETIR e dentre as suas atribuições estão: criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a ETIR; ele será o responsável pela comunicação com o CTIR Gov.

3.4 O Coordenador da ETIR deverá ser designado formalmente.

3.5 A ETIR deverá registrar em uma base de incidentes todos os incidentes em redes computacionais notificados ou detectados.

3.6 Os incidentes em redes computacionais serão classificados como comuns e críticos, conforme a tabela de criticidade definida no processo de gestão de incidentes.

3.7 A ETIR deverá tratar os incidentes em redes computacionais classificados e confirmados como críticos.

3.8 Os incidentes em redes computacionais deverão ser quantificados, classificados e

priorizados para identificar os incidentes recorrentes e os que causam alto impacto ao Ibama.

3.9 Os pontos de contato para enviar informações de incidentes computacionais serão o e-mail etir@ibama.gov.br e a central de atendimento Atende TI (https://atendeti.ibama.gov.br/portal/).

3.10 O Coordenador da ETIR deverá avaliar e validar os incidentes classificados como críticos ou de segurança.

3.11 Durante o tratamento e a resposta ao incidente em redes computacionais a ETIR deverá:

3.11.1 Caso haja indícios de ilícito criminal, coletar e preservar suas evidências o mais rápido possível;

3.11.2 Comunicar os incidentes de segurança, por meio de relatórios, à autoridade responsável na Administração Pública Federal;

3.11.3 Registrar as atividades executadas ao tratar e responder ao incidente para análises futuras;

3.11.4 Comunicar às partes interessadas e aos órgãos externos de tratamento e resposta a incidentes de segurança da informação e comunicações;

3.11.5 Usando o conhecimento adquirido com o incidente, reparar as fragilidades que contribuíram para o incidente e propor aperfeiçoamento ou adição de controles para mitigar o risco de incidentes similares; e

3.11.6 Realizar análises para identificar a origem e a causa do incidente.

3.12 A ETIR será responsável por desenvolver e gerenciar as estratégias de ação e também por receber e fornecer as informações de incidentes de segurança de/para o CTIR Gov, autoridades legais, órgãos da Administração Pública Federal - APF, dentre outros, além de se comunicar com as partes interessadas e correlacionar eventos para identificar tendências e tratar incidentes nos processos monitorados no seu escopo.

3.13 A ETIR deverá comunicar ao CTIR Gov os incidentes de segurança, exceto informações consideradas sigilosas pelo Ibama.

3.14 Os eventos relacionados abaixo, quando não autorizados, serão considerados incidentes de segurança que deverão ser notificados pela ETIR ao CTIR Gov:

3.14.1 Abuso de sítios – desfiguração (defacement), injeção de links/código, spamdexing, erros de código, cross site scripting, abuso de fórum etc.;

3.14.3 Redirecionamento de sítios;

3.14.3 Inclusão de arquivos em servidores;

3.14.4 Uso abusivo de servidores de e-mail;

3.14.5 Ataques de engenharia social – phishing;

3.14.6 Elaboração, distribuição, hospedagem ou redirecionamento de artefatos maliciosos como vírus, malware, bots, rootkits;

3.14.7 Uso ou acesso não autorizado a sistemas ou dados;

3.14.8 Uso impróprio de sistemas (uso de software ou aplicação para práticas ilícitas, tais como pedofilia, pornografia, registro de usuários inexistentes e invasão de sistemas);

3.14.9 Comprometimento de computadores ou redes;

3.14.10 Ataques para roubo de senhas;

3.14.11 Ataques de negação de serviço;

3.14.12 Cópia, exposição ou distribuição de material protegido por direitos autorais;

3.14.13 Cópia, exposição ou distribuição de documentos ou códigos sigilosos;

3.14.14 Varredura de portas; e

3.14.15 Uso abusivo ou indevido de rede ou sistema do Ibama para difamação, calúnia, ameaça ou fraude.

3.15 Durante a gestão de incidentes de segurança, se houver indícios de ilícitos criminais a ETIR deverá:

3.15.1 Informar a presidência do Ibama, que acionará as autoridades policiais competentes para adoção dos procedimentos legais cabíveis; e

3.15.2 Observar os procedimentos previstos no processo de gestão de incidentes para preservação das evidências.

4 MODELO DE IMPLEMENTAÇÃO

4.1 Como modelo de implementação, a ETIR do Ibama adotará o modelo 2, centralizado, da Norma Complementar nº 05/IN01/DSIC/GSIPR, de 2009.

4.1.1 Neste modelo, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais será estabelecida de forma centralizada no âmbito do Ibama.

4.1.2 A Equipe será composta por pessoal com dedicação exclusiva às atividades de tratamento e resposta aos incidentes em redes computacionais.

4.1.3 O Agente Responsável terá, dentre outras atribuições, a de ser a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV. Este Agente será o responsável por criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a Equipe ou Equipes que compõem a ETIR

4.1.4 O Agente Responsável deverá ser designado formalmente.

5 AUTONOMIA

5.1 A ETIR do Ibama terá autonomia completa conforme a Norma Complementar nº 05/IN01/DSIC/GSIPR, de 2009.

5.1.1 Com plena autonomia, a Etir poderá conduzir o seu público alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança. Durante um incidente de segurança, se tal se justificar, a Equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

5.1.2 Em casos emergenciais, havendo grave ameaça à infraestrutura e à segurança da informação do Ibama, a ETIR poderá executar as medidas necessárias para tratar o incidente de segurança, comunicando-as em seguida.

6 ESTRUTURA ORGANIZACIONAL

6.1 Recomenda-se que a ETIR seja composta por: administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede, analistas de suporte ou quaisquer outros agentes públicos do Ibama com conhecimento técnico adequado.

6.2 Deverá haver um substituto para cada membro da ETIR, que deverá ser treinado e orientado para realizar as atividades da ETIR.

6.3 Os integrantes da ETIR deverão reportar-se ao Agente Responsável. A ETIR interagirá internamente com as equipes técnicas do Ibama e externamente com o CTIR Gov, podendo interagir também com outros órgãos similares da Administração Pública Federal – APF, como o Cert.br e o CAIS/RNP.

7 PÚBLICO-ALVO

O público-alvo da ETIR é formado por todos os usuários internos da rede computacional e sistemas do Ibama, incluindo as superintendências regionais e colegiados, e pelos usuários externos que acessam os serviços do Ibama.

8 RESPONSABILIDADES

8.1 São atribuições da Presidência do Ibama, quanto a incidentes em redes computacionais:

8.1.1 Aprovar e instituir o processo de gestão de incidentes;

8.1.2 Aprovar e instituir a norma da ETIR;

8.1.3 Aprovar a estrutura organizacional e as responsabilidades para o processo de gestão de incidentes; e

8.1.4 Aprovar as melhorias para o processo de gestão de incidentes e para a norma da ETIR.

8.2 São atribuições do Comitê de Governança Digital - CGD, quanto à gestão de incidentes em redes computacionais:

8.2.1 Propor as diretrizes gerais do processo de gestão de incidentes e da norma da ETIR;

8.2.2 Propor melhorias para o processo de gestão de incidentes e da norma da ETIR;

8.2.3 Avaliar os indicadores da gestão de incidentes;

8.2.4 Divulgar internamente esta norma.

8.3 São atribuições do Coordenador da Etir:

8.3.1 Coordenar a implementação e manutenção dos recursos materiais e tecnológicos necessários à ETIR;

8.3.2 Propor melhorias para o processo de gestão de incidentes de segurança;

8.3.3 Indicar os cursos para a capacitação dos membros da ETIR em gestão de incidentes em redes computacionais e Segurança da Informação e Comunicações;

8.3.4 Estabelecer procedimentos para evitar o envio de informações sigilosas para órgãos

externos – CTIR Gov e Cert BR – quando ocorrerem incidentes de segurança,

8.3.5 Estabelecer os perfis do Agente Responsável e dos membros da ETIR, e

8.3.6. Indicar, dentre os membros da Etir, o Agente Responsável.

8.4 São atribuições do Agente Responsável da ETIR, quanto aos incidentes em redes computacionais:

8.4.1 Coordenar as ações, distribuir os trabalhos e criar os procedimentos internos da ETIR;

8.4.2 Gerir os incidentes cuja prioridade for classificada como "crítica" ou "alta";

8.4.3 Avaliar a classificação e priorização dos incidentes definidas inicialmente pela central de atendimento Atende TI, validar a existência dos incidentes segurança de sua competência e comunicar ao Coordenador da Etir os incidentes de segurança críticos para validação;

8.4.4 Priorizar os incidentes críticos detectados por ferramentas de monitoramento;

8.4.5 Ser o responsável pela comunicação entre a ETIR do Ibama e o CTIR Gov;

8.4.6 Fornecer os relatórios gerenciais de incidentes para o Coordenador de Etir e à Alta Administração do Ibama;

8.4.7 Buscar eficácia e eficiência do processo de gestão de incidentes;

8.4.8 Buscar a melhoria continua do processo de gestão de incidentes;

8.4.9 Solicitar a criação de planos de contingência para incidentes críticos;

8.4.10 Registrar informações complementares dos incidentes na base de dados;

8.4.11 Monitorar os prazos para resolução dos incidentes críticos;

8.4.12 Definir indicadores para gerenciamento dos incidentes;

8.4.13 Elaborar o modelo de relatório de incidentes contendo:

a) descrição;

b) impacto;

c) tratamento aplicado;

d) vulnerabilidades, ameaças e riscos relativos ao incidente;

e) análise de riscos relativos ao incidente; e

f) planos de contingência propostos; e

8.4.14 Consolidar e enviar ao Coordenador da Etir os relatórios produzidos pela equipe.

8.5 São atribuições dos membros da ETIR, quanto aos incidentes em redes computacionais:

8.5.1 Relacionar e propor recursos materiais e tecnológicos necessários à ETIR;

8.5.2 Registrar as informações sobre as atividades e procedimentos realizados para o tratamento dos incidentes;

8.5.3 Resolver os incidentes de sua competência;

8.5.4 Solicitar informações complementares dos envolvidos nos incidentes;

8.5.5 Monitorar os incidentes de segurança;

8.5.6 Tratar os incidentes;

8.5.7 Gerar relatórios de incidentes;

8.5.8 Propor melhorias para o processo de gestão de incidentes; e

8.5.9 Informar ao Agente Responsável da ETIR sobre os incidentes cujo prazo de resolução esteja perto do fim.

8.6 É atribuição da central de atendimento Atende TI receber as notificações de incidentes em redes computacionais dos usuários do Ibama e classificá-las como requisições, incidentes comuns e incidentes críticos, e como incidentes de segurança.

8.7 É atribuição dos usuários informar a central de atendimento Atende TI por meio de formulários web ou e-mail sobre os incidentes em redes computacionais de seu conhecimento.

9DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas a respeito desta norma serão submetidos ao Comitê de Governança Digital - CGD e à Coordenação-geral de Tecnologia da Informação - CGTI.

10 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO VIII
Norma Complementar 11

Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma	Revisão	Emissão	Folha
11/NC/POSIC/CGD	01	20/09/2021	1
Gestão de continuidade de negócios, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

ORIGEM

Comitê de Governança Digital do Ibama (CGD)

REFERÊNCIA NORMATIVA

- Decreto nº 9.637, de 2018;
- Instrução Normativa 01 GSI/PR, de 13 de junho de 2008;
- Norma Complementar n°06/IN01/DSIC/GSIPR, de 11 de novembro de 2009; ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão de Segurança da Informação;
- ABNT NBR ISO/IEC 27002:2013 – Código de Prática para Controles de Segurança da Informação; ABNT NBR ISO 22313:2020 – Sistema de Gestão de Continuidade de Negócios; e
- ITIL 2011 – Biblioteca de Infraestrutura de Tecnologia da Informação.

CAMPO DE APLICAÇÃO

Esta norma aplica-se no âmbito do Ibama.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta Norma Complementar substitui a NC 11/NC/POSIC/CSII, de 17/04/2015.

Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis			
Número da Norma	Revisão	Emissão	Folha
11/NC/POSIC/CGD	01	20/09/2021	2
Gestão de continuidade de negócios, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

1 CONSIDERAÇÕES INICIAIS

Considerando a necessidade de proporcionar ao Ibama proteção de seus ativos críticos e maior resiliência quanto a interrupções em produtos e serviços; considerando que a Gestão de Continuidade de Negócios – GCN é um processo de melhoria continua que objetiva estabelecer procedimentos, de forma planejada, que minimizem os impactos causados por eventuais interrupções e desastres.

2 OBJETIVO

Estabelecer diretrizes, processos, planos e responsabilidades necessárias para que a gestão de continuidade de negócios do Ibama seja capaz de responder eficazmente às interrupções que venham a ocorrer nos processos de negócios críticos, minimizando assim os impactos causados.

3 CONCEITOS E DEFINIÇÕES

Para o entendimento desta norma, conforme a Política de Segurança da Informação, Informática e Comunicações do Ibama (POSIC), considera-se:

3.1 Ameaça: causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização;

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

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

3.4 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);

3.5 Gestão da 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;

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

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

3.8 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;

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

3.10 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;

4 DIRETRIZES

4.1 Todos os serviços críticos do Ibama e as respectivas unidades de negócios deverão ser identificados e mapeados.

4.2 Os ativos críticos que compõem os serviços críticos dessas unidades de negócios deverão ser identificados, devendo existir pelo menos um proprietário ou responsável por ativo crítico.

4.3 Análises de risco deverão ser executadas para os ativos críticos existentes.

4.4 Os riscos analisados deverão ser tratados e este processo deverá estar em conformidade com a matriz de tratamento de riscos utilizada pela Norma Complementar nº 06 - Gestão de Riscos de Segurança da Informação do Ibama.

4.5 Deverão ser analisados os impactos causados nos negócios pela eventual indisponibilidade de serviços críticos.

4.6 Os prazos de indisponibilidade, as estratégias para a continuidade e recuperação dos serviços críticos deverão ser documentados.

4.7 O Plano de Continuidade de Negócios – PCN, deverá conter os seguintes itens:

4.7.1 Objetivo e escopo;

4.7.2 Papéis e responsabilidades;

4.7.3 Autoridade responsável;

4.7.4 Detalhes de contato;

4.7.5 Lista de tarefas; e

4.7.6 Recursos necessários.

4.8 Deverá ser elaborado o cronograma de testes para execução do plano de continuidade de negócios

4.9 Os contratos firmados com empresas terceirizadas que suportem atividades críticas devem conter cláusula que exija das referidas empresas os planos de continuidade dos seus negócios, bem como as evidências dos testes realizados.

5 RESPONSABILIDADES

5.1 São atribuições da Presidência do Ibama:

5.1.1 Aprovar a norma de continuidade de negócios;

5.1.2 Aprovar as diretrizes para o programa de continuidade de negócios;

5.1.3 Avaliar a relação custo/benefício das estratégias de continuidade propostas e do plano de continuidade de negócios;

5.1.4 Aprovar o plano de continuidade de negócios;

5.1.5 Aprovar a realização dos testes para comprovar a eficácia do plano.

5.2 São atribuições do Comitê de Governança Digital (CGD) avaliar a norma de continuidade de negócios;

5.2.1 Avaliar as diretrizes para o plano de continuidade de negócios;

5.2.2 Avaliar o plano de continuidade; e

5.2.3 Avaliar as datas definidas para realização dos testes.

5.3 São atribuições da Coordenação-Geral de Tecnologia da Informação (CGTI):

5.3.1 Fomentar os recursos necessários para estabelecer, implementar, operar e manter o plano de continuidade de negócios;

5.3.2 Fomentar a cultura de gestão de continuidade de negócios; III – identificar e mapear os ativos/serviços críticos;

5.3.3 Identificar e mapear os proprietários dos ativos/serviços críticos.

5.4 São atribuições do Gestor de Segurança da Informação:

5.4.1 Propor as diretrizes para o programa de continuidade de negócios;

5.4.2 Avaliar o plano de tratamento de riscos;

5.4.3 Supervisionar a elaboração, implementação, testes e atualização dos planos que compõem o programa de continuidade de negócios;

5.4.4 Tomar conhecimento do plano de gestão de incidentes e gestão de crises; e

5.4.5 Contactar as partes interessadas quando da realização dos testes que validarão os planos.

5.5 São atribuições da equipe de continuidade de negócios:

5.5.1 Elaborar, implementar, testar e atualizar os planos que compõem o plano de continuidade de negócios;

5.5.2 Validar com os proprietários dos ativos/serviços críticos o plano de continuidade de negócios; e

5.5.3 Validar com os proprietários dos ativos/serviços críticos os testes que validarão o plano elaborado.

5.6 São atribuições dos proprietários dos ativos/serviços críticos:

5.6.1 Definir os prazos máximos de indisponibilidade dos ativos/serviços críticos;

5.6.2 Auxiliar a equipe de continuidade de negócios na elaboração, validação e revisão do plano de continuidade de negócios;

5.6.3 Auxiliar a equipe de continuidade de negócios na elaboração, validação e revisão dos testes que validarão o plano elaborado;

5.6.4 Definir as datas para realização dos testes; e

5.6.5 Validar e confirmar a operacionalização do ativo/serviço crítico após o término da indisponibilidade.

5.7 É atribuição das equipes técnicas do Ibama reestabelecer ou recuperar os serviços críticos afetados.

6 DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas a respeito desta norma serão submetidos ao Comitê de Governança Digital - CGD e à Coordenação-geral de Tecnologia da Informação - CGTI.

7 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO IX
Norma Complementar 12

IBAMA MMA	**Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis**			
Número da Norma	Revisão	Emissão	Folha	
12/NC/POSIC/CGD	00	20/09/2021	1	
Gestão dos serviços terceirizados, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC				

ORIGEM

Comitê de Governança Digital do Ibama (CGD)

REFERÊNCIA NORMATIVA

- Lei n° 8.666, de 21.06.1993 - Lei de Licitações e Contratos Administrativos
- Lei n° 13.709, de 14.08.2018 - Lei Geral de Proteção de Dados Pessoais - LGPD

- Instrução Normativa nº 5, de 26.05.2017 - Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.

CAMPO DE APLICAÇÃO

Esta norma aplica-se no âmbito do Ibama.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

IBAMA MMA	Ministério do Meio Ambiente Instituto do Meio Ambiente e dos Recursos Naturais Renováveis		
Número da Norma	Revisão	Emissão	Folha
12/NC/POSIC/CGD	00	20/09/2021	2
Gestão dos serviços terceirizados, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

1 OBJETIVO

Estabelecer diretrizes e responsabilidades necessárias para a gestão dos serviços terceirizados no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC do Ibama.

2 CONCEITOS E DEFINIÇÕES

Para efeito desta norma considera-se:

2.1 Atividades autorizadas: acesso de terceiros a informações e ativos do Ibama.

3 DIRETRIZES

3.1 Todo acesso a informações e ativos do Ibama somente serão autorizadas após regular preenchimento de termo de responsabilidade.

3.2 São atividades autorizadas para acesso e manuseio por terceiros.

3.2.1 Os serviços de limpeza e conservação.

3.2.2 Os serviços de brigada e segurança.

3.2.3 Os serviços de manutenção predial.

3.2.4 Os serviços de copeiragem.

3.2.5 Serviços de apoio administrativo.

3.3 Os serviços terceirizados contratados por esta Autarquia, ocorrerão segundo a IN n° 05, de 26.05.2017 SEGES/MPOG.

3.4 Toda atualização da Política de Segurança da Informação e Comunicações do Ibama - POSIC 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 necessárias à Autarquia.

3.5 Os colaboradores do Ibama que utilizam os recursos de TIC (Tecnologia da informação e Comunicação) terão uma conta de acesso, pessoal e intrasferível.

3.6 As permissões de acesso aos recursos de tecnologia e informação serão concedidas aos colaboradores terceirizados conforme necessidade dos setores.

3.7 Aos agentes terceirizados das áreas de: copeiragem, limpeza, conservação, e manutenção predial, serão concedidos acessos aos sistemas digitais da entidade conforme demanda dos setores.

3.8 Os agentes terceirizados da brigada e segurança, terão acesso aos sistemas referentes a controle de acesso, vigilância e circuito e câmeras.

4 RESPONSABILIDADES

4.1 São responsabilidades dos agentes de vigilância e brigada, quando locados na portaria central do Ibama:

4.1.1 Realizar controles de acesso à Autarquia, que envolvem: identificação, cadastro e quando necessário, revista.

4.1.2 Agir de forma preventiva e pro-ativa a fim de prevenir e obstruir ações adversas de qualquer natureza contra pessoal, áreas, instalações e materiais do Ibama.

4.1.3 Monitorar a entrada e a saída de veículos, sejam esses de agentes do Ibama ou de particulares.

4.1.4 Operar a sala de monitoramento.

4.2 Os relacionamentos contratuais do Ibama de serviços terceirizados são fundamentados na Lei n° 8.666, de 21.06.1993 e na IN n° 05, de 26.05.2017 SEGES/MPOG.

4.2.1 Contratos firmados pelo Ibama conterão cláusulas que determinem a observância das diretrizes estabelecidas pela POSIC.

4.2.2 As empresas prestadoras de serviço deverão conhecer e cumprir a nas normas estabelecidas pela POSIC.

4.2.3 Toda atualização da POSIC do Ibama bem como de procedimentos, sistemas e processos envolvidos deverão ser repassados as empresas prestadoras de serviço.

5 DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas a respeito desta norma serão submetidos ao Comitê de

Governança Digital - CGD e à Coordenação-geral de Administração - CGEAD.

6 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO I

TERMO DE RESPONSABILIDADE DE ACESSO A INFORMAÇÃO E DADOS

Pelo presente termo de responsabilidade, eu_____, CPF N° _____e RG N° _____, comprometo-me com a adequada utilização das informações a que tiver acesso durante o exercício das

atividades laborais desempenhadas por este colaborador junto ao Ibama, em conformidade a Lei N° 13.709, de 14 de agosto de 2018, sob pena de responder nas esferas penal, civil e administrativa, pelo descumprimento das regras estabelecidas ou prática de condutas ilícitas pelo mau uso das informações disponibilizadas, estando ciente quanto a segurança e tratamento adequado das informações, em especial:

1. Todas as informações adquiridas durante o exercício de funções laborais deverão estar em conformidade com a Lei 13.709/2018.
2. São normas gerais da lei de proteção de dados observadas por este órgão: respeito a privacidade, inviolabilidade da intimidade, da honra e da imagem.
3. É vedado o compartilhamento dos dados adquiridos, sejam eles de agentes públicos ou de terceiros.
4. Toda informação gerada, adquirida, utilizada ou armazenada, durante o exercício das atividades laborais junto ao Ibama, é classificada como patrimônio do Ibama.
5. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento, por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior do Ibama.

Cidade/UF, ____de_____de

_____

Assinatura

ANEXO X
Norma Complementar 13

	Ministério do Meio Ambiente **Instituto do Meio Ambiente e dos Recursos** **Naturais Renováveis**		
Número da Norma	Revisão	Emissão	Folha
13/NC/POSIC/CGD	00	20/09/2021	1
Processo de Gestão de Riscos de Segurança da Informação, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

ORIGEM

Comitê de Governança Digital do Ibama (CGD)

REFERÊNCIA NORMATIVA

- Instrução Normativa 01 GSI/PR, de 13 de junho de 2008; Instrução Normativa 03 GSI/PR, de 28 de maio de 2021;
- ABNT NBR ISO/IEC 27005:2019 - Gestão de riscos de segurança da informação; ABNT NBR ISO 31000:2018 - Gestão de riscos - Diretrizes;
- ABNT ISO/IEC 27002:2013 – Código de Prática para Controles de Segurança da Informação; ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão da Segurança da Informação;
- ABNT ISO GUIA 73:2009 - Gestão de riscos - Vocabulário; e
- ISO/IEC 27000:2018 - Especifica conceitos e definições relacionados às normas de segurança da informação

CAMPO DE APLICAÇÃO

-

Esta norma aplica-se no âmbito do Ibama.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

Número da Norma	Revisão	Emissão	Folha
13/NC/POSIC/CGD	00	20/09/ 2021	2
Processo de Gestão de Riscos de Segurança da Informação, no âmbito da Política de Segurança da Informação, Informática e Comunicações - POSIC			

1 OBJETIVO

Estabelecer as diretrizes da gestão de riscos relacionada ao ambiente tecnológico no âmbito deste Instituto, aos projetos e processos de Tecnologia da Informação e Comunicações (TIC), e definir o processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações do Ibama (GRSIC-Ibama).

2 CONCEITOS E DEFINIÇÕES

Para o entendimento adequado desta Norma, em conformidade com a POSIC, considera-se:

2.1 Ameaça - causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização;

2.2 Análise de riscos - processo para compreender a natureza do risco e determinar o nível de risco;

2.3 Avaliação de riscos - processo de comparação dos resultados da análise de risco com critérios de risco para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis;

2.4 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;

2.5 Comunicação do risco - conjunto de processos continuos e iterativos que uma organização realiza para fornecer, compartilhar ou obter informações e para dialogar com as partes interessadas sobre o gerenciamento de riscos;

2.6 Estimativa de riscos - processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

2.7 Evitar risco - forma de tratamento de risco pela qual se decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

2.8 Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC–Ibama) – conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

2.9 Gestão de Riscos em Projetos de TIC – conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto.

2.10 Gestão de Riscos em Processos de TIC – conjunto de atividades, estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos.

2.11 Identificação de riscos – processo para localizar, listar e caracterizar elementos do risco.

2.12 Reduzir risco – forma de tratamento de risco pela qual se decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

2.13 Reter risco – forma de tratamento de risco pela qual se decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

2.14 Riscos de Segurança da Informação e Comunicações – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

2.15 Transferir risco – uma forma de tratamento de risco pela qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

2.16 Tratamento dos riscos – processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

2.17 Vulnerabilidade - fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

3 DIRETRIZES

3.1 A Gestão de Riscos leva em consideração as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TIC e está alinhada à Política de Segurança da Informação, Informática e Comunicações - POSIC.

3.2 A Gestão de Riscos é abordada de forma sistemática, com o objetivo de manter os riscos em níveis aceitáveis para cada projeto, processo e/ou serviço analisado.

3.3 Os riscos são analisados e avaliados em função de sua relevância para os principais processos de negócio deste Instituto e são tratados de forma a assegurar respostas tempestivas e efetivas.

4 GESTÃO DE RISCOS EM PROJETOS DE TIC

As atividades inerentes ao gerenciamento de riscos em projetos relacionados à TIC devem observar o disposto na metodologia de gerenciamento de projetos adotada pela Coordenação-geral de Tecnologia da Informação - CGTI.

5 GESTÃO DE RISCOS EM PROCESSOS DE TIC

5.1 A gestão e a comunicação de riscos em processos de TIC são definidas na especificação de cada processo e visam à identificação e ao controle dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria. As atividades inerentes à gestão de riscos nos processos de TIC devem observar as diretrizes desta norma e outras específicas relacionadas ao processo.

5.2 A gestão de riscos em processos de TIC é monitorada pela Coordenação-geral de Tecnologia da Informação - CGTI. (item alterado pela Portaria n° 7.137/2017 e pela Portaria nº 6.493/2019)

6 GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (GRSIC-IBAMA)

6.1 O processo de GRSIC-Ibama é continuo, fornecendo subsídios e integrando-se à implantação e operação do Sistema de Gestão de Segurança da Informação.

6.2 O processo de GRSIC-Ibama está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2019 e ABNT NBR ISO/IEC 31000:2018 e na Instrução Normativa 03 GSI/PR, de 28 de maio de 2021.

6.3 Os critérios para avaliação do risco levam em consideração o "PSR": Probabilidade, que é a possibilidade de uma vulnerabilidade ser explorada por uma ou mais ameaça(s), ocasionando um incidente de segurança; Severidade, que é a consequência para o ativo de informação caso um incidente ocorra; e Relevância, que é a importância do ativo de informação para os processos de negócio aos quais ele está relacionado. Desta forma, a avaliação de riscos é realizada através do produto de três variáveis (probabilidade, severidade e relevância). A partir do valor obtido, o risco é classificado de acordo com a tabela a seguir:

Classificação do Risco	Valores do "PSR"
Muito baixo	1 a 6
Baixo	8 a 16
Médio	18 a 30
Alto	32 a 50
Muito baixo	60 a 125

6.4 O tratamento dos riscos será definido de acordo com as necessidades levantadas pelas partes interessadas, regulamentações e legislações vigentes, avaliação técnica e análise custo/benefício.

6.5 O processo de GRSIC-Ibama é composto pelas etapas descritas a seguir:

6.5.1 Contextualização - compreende a definição e aprovação do contexto da análise e avaliação de riscos a ser realizada, com a identificação de seu propósito, escopo, limites e partes interessadas.

6.5.2 Análise e Avaliação dos Riscos - compreende o mapeamento dos ativos, identificação, análise e avaliação dos riscos, bem como a elaboração e aprovação do Plano de Tratamento dos Riscos.

6.5.3 Tratamento dos Riscos - compreende a implementação das ações do Plano de Tratamento de Riscos, seu monitoramento e apresentação dos resultados.

6.5.4 Melhoria continua - compreende a realização da análise crítica pela Administração, com avaliação dos resultados e das propostas de melhoria apresentadas.

7 DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas a respeito desta norma serão submetidos ao Comitê de Governança Digital - CGD e à Coordenação-geral de Tecnologia da Informação - CGTI.

8 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

EDUARDO FORTUNATO BIM